NETGEAR

ProSafe 16 AP Wireless Management System WMS5316

Reference Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

July 2010
202-10601-02
v1.0

©2010 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10601-02	v1.0	July 2010	New document template
202-10601-01	v1.0	March 2010	Original publication

Table of Contents

Chapter 1 Getting Started

Logging In 6
Basic System Settings 7
General Settings 7
Time Settings 8
IP Settings 9
VLAN Settings 9
DHCP Server Settings 11
Syslog Settings 12

Chapter 2 Access Point Discovery

Auto Discovery 13
IP Discovery 14
Discovery Results 15
Adding Access Points 16

Chapter 3 Wireless Configuration

Configuring Centralized RF Management 17
Advanced Wireless Settings for Access Point Groups 18
Configuring QoS 21
QoS for Managed Access Points 21
Advanced QoS Settings for Access Point Groups 22
Load Balancing 22
Load Balancing for Managed Access Points 23
Advanced Load Balancing for Access Point Groups 23

Chapter 4 Security Configuration

Security Profiles Lists 24
Security Profiles List for Access Points 24
Editing a Security Profile 25
Advanced Security Profiles List for Access Point Groups 26
Rogue Access Points 27
MAC Authentication 28
MAC Authentication for Access Points 29
Advanced MAC Authentication for Access Point Groups 29
Radius Server Settings 31
Configuring Guest Access 32

Guest Access Show 33

Chapter 5 Monitoring

Monitoring Summary 34
Access Point Status 34
Rogue Access Points 35
Wireless Stations 35
Network Info 35
Network Usage 36
Access Point Status 36
Access Point Status Details 37
Client Status 38
Network Usage 39
Network Usage Statistics 39
Network Topology 39
DHCP Leases 40
Monitoring Rogue Access Points 40

Chapter 6 Configuring Access Point Groups

Managed Access Point List 42
Editing Access Point Information 43
IP Settings 44
Access Point Groups 44

Chapter 7 Maintenance

User Management 45
Changing Passwords 46
Reset 46
Rebooting the Wireless Management System 46
Restoring Factory Default Settings 47
Rebooting an Access Point Group 48
SNMP 48
SNMP for the Wireless Management System 48
SNMP for Access Point Groups 49
Remote Management 50
Remote Console for the Wireless Management System 50
Advanced Remote Console for Access Point Groups 50
Session Timeout 51
Upgrading the Firmware 51
Upgrading the Wireless Management System Firmware 51
Upgrading Access Point Firmware 52
Backing Up Configuration Settings 54
Restoring Settings from a File 54
Downloading Wireless Management System Logs 55
System Logs 55

Access Point Logs 56
Diagnostic Ping Screen 56
Using Discovery OUI 57

Appendix A Access Point Firmware Compatibility

Compatible Access Point Supported Firmware Versions 58
Controller Features and Access Point Compatibility 59

Appendix B Factory Default Settings

Appendix C Notification of Compliance

Index

Getting Started

1

The ProSafe 16 AP Wireless Management System allows you to manage up to 16 NETGEAR wireless access points on a LAN. You can use the wireless management system to:

- Discover NETGEAR access points on the LAN.
- Optimize wireless access point performance with centralized RF management, QoS, and load balancing.
- Streamline security configuration tasks and set up guest access.
- Monitor network usage.
- Perform maintenance tasks including user management, remote management, and firmware updates for the wireless management system and for NETGEAR access points on the LAN.

Depending on your network configuration, you can use basic settings or advanced settings to manage your access points:

- **Basic Settings for a typical network**: The basic settings work with the most common network configuration. All access points on the LAN are for the same organization or business.
- **Advanced Settings for access point groups**: If completely separate networks share a single LAN, use the advanced settings to set up access point groups. For example, a shopping mall might need access point groups if several businesses share a LAN, but each business has its own network.

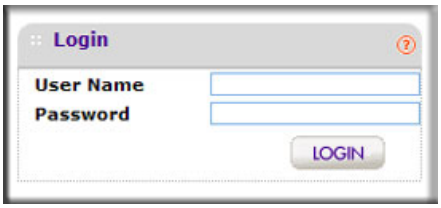
Logging In

Note: For help installing the ProSafe 16 AP Wireless Management System, see the *Installation Guide* included in the package and on the *Resource CD*.

To log in to the wireless management system you must use a computer that is configured with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0. Connect the computer to a LAN port on the wireless management system with an Ethernet cable.

1. In the address field of your Internet browser, type the IP address for the ProSafe 16 AP Wireless Management System. Its default IP address is **http://192.168.0.250**.

   A login prompt displays:



2. If you are logging in for the first time, use the default user name **admin** and password (**password**).

   NETGEAR recommends that you change the password to a new, more secure password and record it in a secure location.

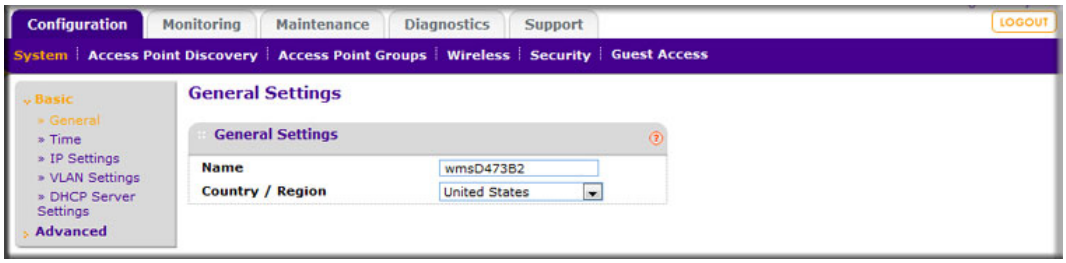
   The user interface opens with the Configuration tab selected. This tab is shown in the following section, Basic System Settings.

Basic System Settings

When you log in, the Configuration tab displays General Settings.

General Settings

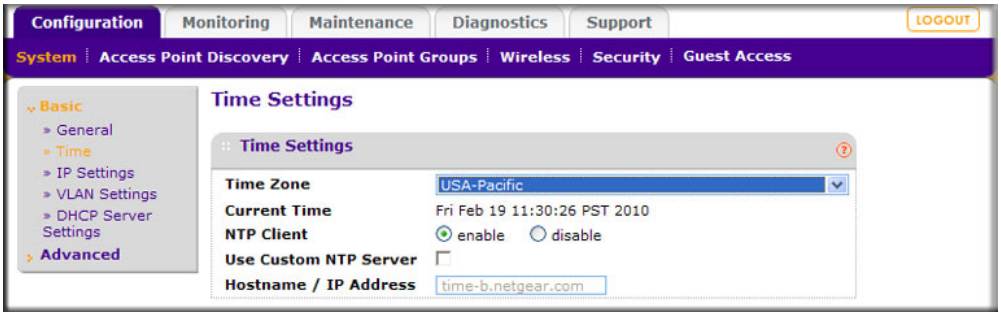
To navigate to this screen, on the Configuration tab select System > Basic > General:



The General Settings screen lets you configure the basic settings of your wireless management system.

- **Name**: This unique value indicates the wireless management system name. By default, the name is wms5316.

  NETGEAR recommends changing the name as soon as possible after setting up. The name must contain only alphabetical characters, numbers, and hyphens, and must be 31 characters or less.



- **Country/Region**: This field displays the region of operation for the wireless management system and the access points managed by the wireless management system. In the United States, the country is preset and cannot be changed on the access points. If the country/region is not set up correctly, the wireless management system might not be able to access the access points.

For products sold outside the United States, you must select a country or region. It might not be legal to operate the access points in a country/region not shown here. If your location is not listed, check with your local government agency or check the NETGEAR website for more information about which channels to use.

Time Settings

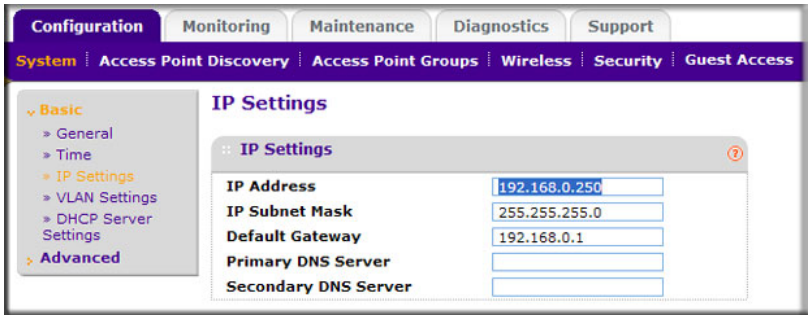
On the Configuration tab, select System > Basic > Time Settings:

This screen lets you configure the time-related settings of your wireless management system and managed access points. It has the following options:

- **Time Zone**: Select the local time zone for your region or country.
- **Current Time**: The current time at your location.
- **NTP Client**: Enable this to use a Network Time Protocol (NTP) server to synchronize the clock of the wireless management system and managed access points. Disable this option if you do not want to use an NTP server.
- **Use Custom NTP Server**: Select this check box if you wish to use an alternate NTP server. By default, the NETGEAR NTP server is used by the access point.
- **Hostname / IP Address**: Provide the host name or IP address of the NTP server, if you are using a custom NTP server.

IP Settings

On the Configuration tab select System > Basic > IP Settings:

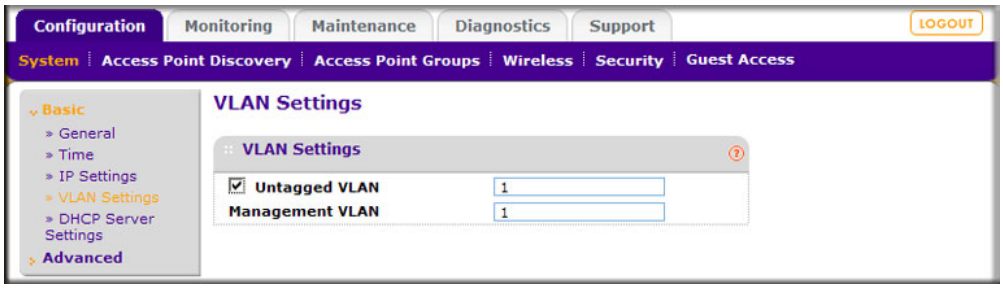


This screen lets you to configure the management IP address settings of the wireless management system. It has the following options:

- **IP Address**: This is the IP address of the wireless management system. The default IP address is 192.168.0.250. To change it, enter an available IP address from the address range used on your LAN.
- **IP Subnet Mask**: Enter the subnet mask value used on your LAN. The default value is 255.255.255.0.
- **Default Gateway**: Enter the IP address of the gateway for your LAN.
- **Primary DNS Server**: Enter the IP address of the primary Domain Name Server (DNS) that you want to use.
- **Secondary DNS Server**: Enter the IP address of the secondary DNS that you want to use.

VLAN Settings

To go to VLAN settings, click the Configuration tab, and select System > Basic > VLAN Settings.



The 802.1Q VLAN protocol on the wireless management system logically separates traffic on the same physical network. The settings apply only to the wireless management system.

Untagged VLANs

When the **Untagged VLAN** check box is selected, one VLAN can be configured as an untagged VLAN.

For each profile group up to 8 VLANS can be configured per radio, for example, a maximum of 15 SSIDs per group for both the radios. The active VLANs depend on the active SSIDs and access points that are deployed. If the access point is a ProSafe dual band, such as the WNDAP350, then all 16 can be active. If it is a ProSafe single band, then only 8 SSIDs can be active. If it is a SoHo access point, then only one SSID can be active.

The wireless management system itself can support 2 VLANs, one management VLAN and one untagged VLAN.

When the wireless management system sends frames associated with the untagged VLAN out the LAN (Ethernet) interface, those frames are untagged. When the wireless management system receives untagged traffic from the LAN (Ethernet) interface, those frames are assigned to the untagged VLAN.

If this check box is cleared, the wireless management system tags all outgoing LAN (Ethernet) frames, and accepts only incoming frames that are tagged with known VLAN IDs.

> **Note:** The **untagged VLAN** check box should be cleared only if the hubs or switches on your LAN support the VLAN (802.1Q) standard. Likewise, the untagged VLAN value should be changed only if the hubs and switches on your LAN support the VLAN (802.1Q) standard.

Changing either of these values will result in a loss of IP connectivity if the hubs and switches on your network have not yet been configured with the corresponding VLANs.

The **Untagged VLAN** check box must be cleared when either access point model WN802Tv2 or access point model WG602v4 is managed, as those access points do not support 802.1Q VLAN tagging.

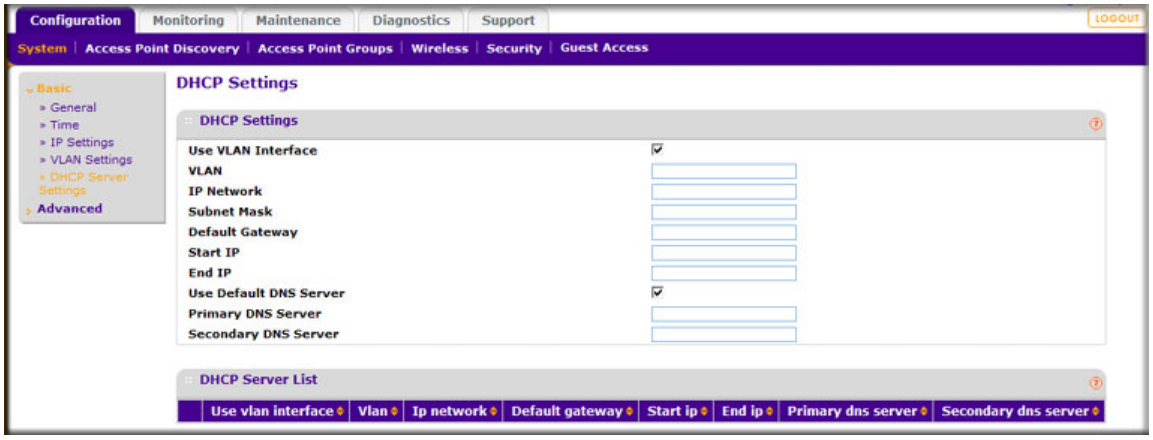
Management VLANs

Management VLANs are used for managing traffic (Telnet, SNMP, and HTTP) to and from the wireless management system and managed access points.

Frames belonging to the management VLAN are not given any 802.1Q header when sent over the trunk. If a port is in a single VLAN, it can be untagged. But if the port needs to be a member of multiple VLANs, it must be tagged.

DHCP Server Settings

The wireless management system can function as a DHCP server. Multiple DHCP server pools can be added for different VLANs. Click the Configuration tab and select System > Basic > DHCP Server Settings to display the following screen:



This screen lets you to enable and configure the DHCP server. You can specify the following information:

- **Use VLAN Interface**: Select this check box to enable the wireless management system to provide IP addresses to clients in a specified VLAN.

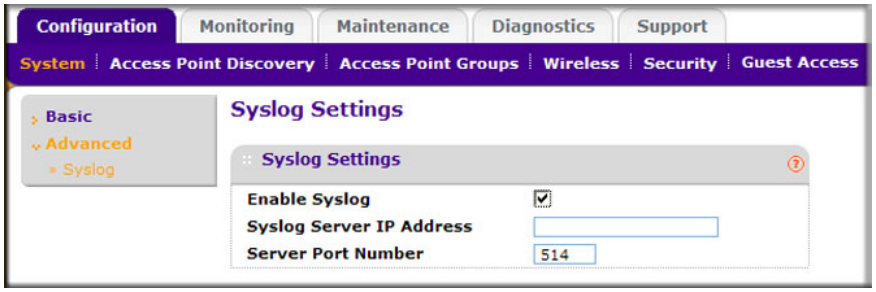
> **Note:** Selecting the **Use VLAN Interface** check box allows you to access the VLAN IP Address and Subnet Mask fields. Select this option if the DHCP pool being added is only for a particular VLAN.

- **VLAN**: Enter the DHCP server VLAN ID. The range is between 1 and 4094. The DHCP server will service this VLAN.
- **IP Address**: The IP address for the wireless management system in the specified VLAN; when the **Use VLAN Interface** check box is not selected, the wireless management system management IP/VLAN is used.
- **Subnet Mask**: Enter the subnet mask that will be assigned to the wireless clients by the DHCP server.
- **Default Gateway**: Enter the IP address of the default network gateway for all traffic beyond the local network.
- **Start IP**: Enter the starting IP address of the range that can be assigned by the DHCP server.
- **End IP**: Enter the ending IP address of the range that can be assigned by the DHCP server.
- **Use Default DNS Server**: Select this check box to allow the wireless management system DNS server to be provided to the clients of the specified VLAN.

- **Primary DNS Server**: Enter the IP address of the primary DNS server for the network.
- **Secondary DNS Server**: Enter the IP address of the secondary DNS server for the network.
- **DHCP Server List**: This displays DHCP server configuration for all configured VLANs.

Syslog Settings

This screen lets you configure the settings to connect to a syslog server, if you have one configured in your network. Click the Configuration tab and select System > Advanced.



- **Enable Syslog**: Enable the syslog settings, if you have a syslog server on your network.
- **Syslog Server IP Address**: Enter the IP address to which the wireless management system and managed access points will send all syslogs, if the Syslog option is enabled.
- **Server Port Number**: Enter the number of the port at which your syslog server is configured to listen to requests.

Access Point Discovery

2

You can discover supported NETGEAR access points on the LAN that can be managed by the wireless management system. See Appendix A, *Access Point Firmware Compatibility* for a list of compatible access points. The wireless management system supports Auto Discovery and IP Discovery.

- **Auto Discovery**: Use this feature if the wireless management system and all access points on the LAN are in the same IP subnet. This is a Layer 2 discovery method.
- **IP Discovery**: If the wireless management system and access points use different IP subnets, you can use IP discovery to find the access points for each subnet (one subnet at a time). This is a Layer 3 discovery method.

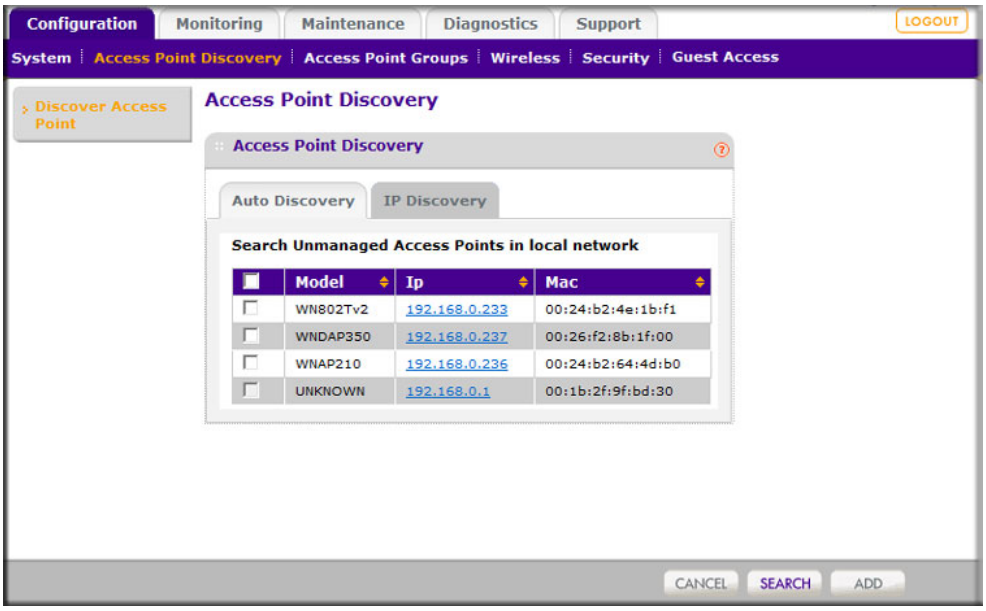
Note: For discovery to work, each access point must have an IP address. If more than one access point has the same default IP address, then only one of them is discovered with the model number at a time. You have to add the access point to the managed list, change its IP address, and then run discovery again to discover the next access point with the default IP.

Auto Discovery

Use Auto Discovery if the wireless management system and all access points on the LAN are in the same IP subnet. The process of Auto Discovery depends on how your access points are configured.

To use Auto Discovery:

1. On the Configuration tab select Access Point Discovery.



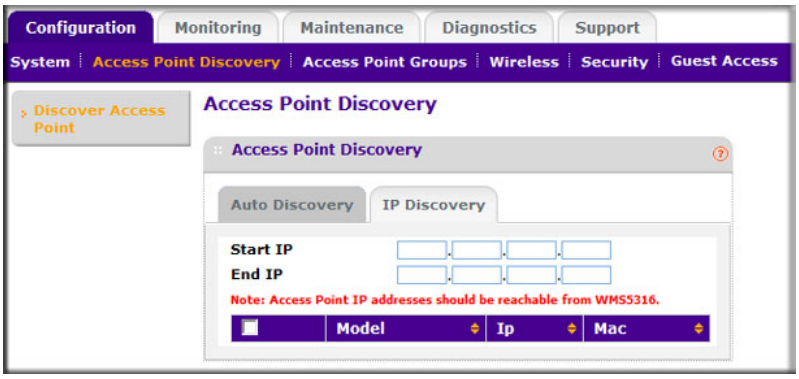
2. Click **Search**.
   - The wireless management system searches for NETGEAR products on the LAN based on MAC address, and then identifies which are access points.
   - A list of the access points located through discovery is displayed on the screen.
3. Check the discovery results to make sure that all the access points are listed. See *Discovery Results* on page 15.
4. Add the access points as described in *Adding Access Points* on page 16.

IP Discovery

Use IP Discovery to discover access points in a different IP network from the wireless management system. You can search for a maximum of 255 IP addresses at a time. NETGEAR recommends that you split up your search if you have access points in multiple networks.

To use IP Discovery:

1. On the Configuration tab select Access Point Discovery, and then click the IP Discovery tab:



2. To specify the range of IP addresses, fill in the **Start IP** and **End IP** fields.
3. Click **Search**.
   - The wireless management system locates devices on the LAN within the range of IP addresses that you specified.
   - The devices are displayed in a list.
4. Check the discovery results to make sure that all the access points are listed. See *Discovery Results* on page 15.
5. Add the access points as described in *Adding Access Points* on page 16.

Discovery Results

The effectiveness of the discovery feature depends in part on how the access points on your LAN are set up. If each access point is configured with a unique IP address and is running current firmware, then discovery is usually simple.

If the discovery results are not what you expect, check the following:

- Access points already managed by the wireless management system are not in the discovery list.
- If two or more access points still have their factory default settings, their IP addresses might be identical. If this is the case, the wireless management system discovers one of these access points. Add that access point, change its IP address, and then use discovery to find the next access point.
- If discovery results show unknown access points, it could be due to these reasons:
  - The access point is running an older version of firmware. Upgrade firmware as needed so that discovery can locate the access point.
  - The wireless management system located a NETGEAR access point that is not supported or located a NETGEAR device that is not an access point.

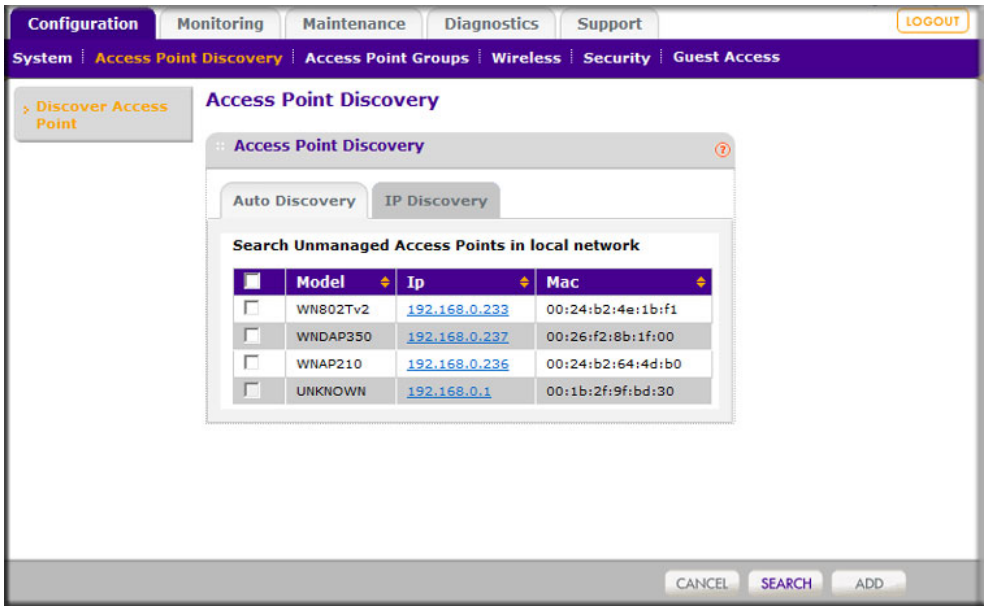
For a list of compatible access point models and their supported firmware, see Appendix A, *Access Point Firmware Compatibility*.

- If a new NETGEAR access point is not discovered, it might have a MAC address that the wireless management system does not recognize, though this is not common. See *Using Discovery OUI* on page 57.

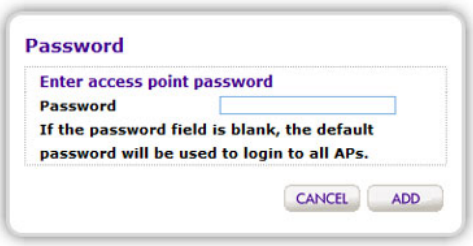
Adding Access Points

After the wireless management system discovers the access points, add them so that they can be managed by the wireless management system.

1. On the Access Point Discovery screen, select the access point and click **Add**.



2. Enter a password for the access point.


Password
Enter access point password
Password
If the password field is blank, the default password will be used to login to all APs.
CANCEL
ADD

Wireless Configuration

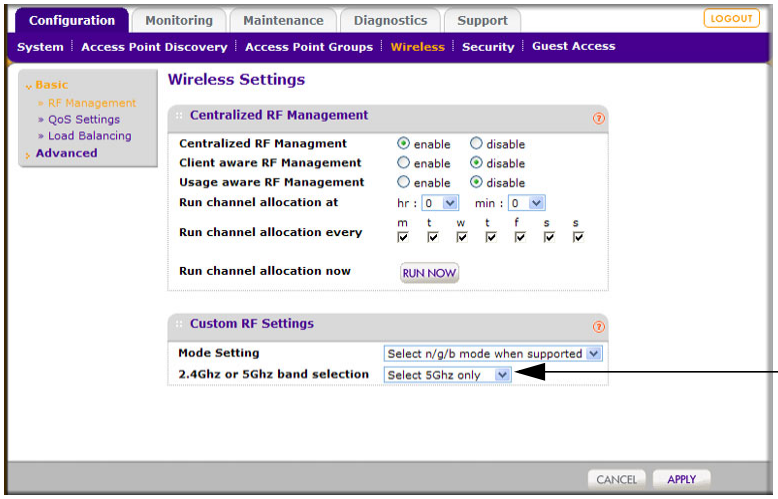
3

You can configure centralized RF management and specify wireless settings in the Basic RF Management screen. If you use access point groups, you can use the Advanced Wireless Settings screen to customize wireless settings for each group.

Configuring Centralized RF Management

In this screen you can specify RF management settings. RF management, when run, optimizes the channel allocation for access points based on clients, user data traffic, and observed nearby RF environment of access points.

On the Configuration tab, select Wireless:



This field applies only to model WNDAP330.

1. Specify the centralized RF management:
   - **Centralized RF Management**: The **Enable** radio button is selected by default. This allows the wireless management system to allocate access point channels based on the access point performance in the local environment. For example, if an access point experiences interference on a channel, the wireless management system allocates a different channel to that access point.

- **Client aware RF Management**: If this **Enable** radio button is selected, the wireless management system does not modify the channel for an access point with associated clients that would be impacted by the channel change. The wireless management system waits for the next scheduled channel allocation to adjust the channel.
- **Usage aware RF Management**: If this **Enable** radio button is selected, the wireless management system does not modify the channel for an access point that is switching more than 1 Mbps of wireless data traffic.
- **Run Channel Allocation at**: Specify at what time of the day the channel allocation can modify access point RF configuration.
- **Run Channel Allocation every**: Specify a weekly schedule for running channel allocation.
- **Run Channel Allocation now**: Click the **Run Now** button to run channel allocation immediately.

2. Enter the custom RF settings:
   - **Mode Settings**: Specify the radio mode preference to set on the access points.

     Most access points are configured with the fastest mode by default. You can use the **Mode Settings** field to change this. For example, you could specify that an access point that supports wireless-n mode run in b/g mode in order to support clients that do not support wireless n technology.
   - **2.4GHz or 5GHz band selection**: This selection affects only dual band access points that can be set to only one band at a time, such as the WNDAP330. You can use this field to specify which band the access point should use.

Note: For dual concurrent access points, both radio modes are enabled by default.

3. Click **Apply** so that your changes take effect.

Advanced Wireless Settings for Access Point Groups

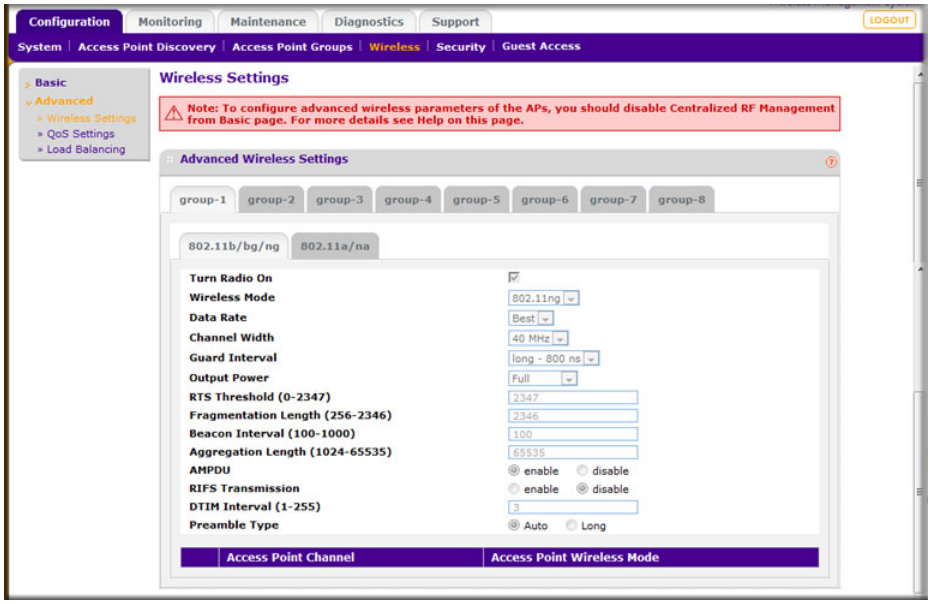
This screen is for advanced users who wish to control the WLAN settings of the access points manually.

To manually specify the WLAN parameters for access points:

1. On the Configuration tab, select Basic > RF Management screen, and disable the Central RF Management on the Wireless Settings screen.

   This prevents the wireless management system from automatically using RF management and adjusting power and channel settings for the access point group.

2. On the Configuration tab, select Advanced > Wireless Settings:



3. Specify the settings in this screen (see Table 1, *Advanced Wireless Settings* for a description of the fields).
4. Click **Apply** so that your changes take effect.

Table 1. Advanced Wireless Settings

Turn Radio On	Disable this option to disable wireless access for the selected mode. To disable all wireless access through this access point, you must turn off the 802.11b/g/n, as well as the 802.11a/n radios.
Wireless Mode	Specify the wireless mode for the access points. Access points use the mode enabled for the group, unless the access point does not support the group setting. In that case, the access point uses the mode providing highest performance. • The default setting is 802.11ng mode. • If you specify 802.11b or 802.11bg mode, both 802.11n- and 802.11g-compliant devices can be used with this access point. However, 802.11b devices will not be able to connect. • If you select this option and other settings on this screen are disabled, then you must select the **Turn Radio On radio** check box to enable available options on this screen.
MCS Index/Data Rate	Select the available transmit data rates of the wireless network.
Channel Width (11n only)	Select the available channel width of the access point. A wider channel improves the performance, but some legacy devices can operate only on either 20 MHz or 40 MHz.
Guard Interval (11n only)	Select the value that will protect transmissions from interference. A shorter guard interval improves performance, but some legacy devices can operate only with a long guard interval.

Table 1. Advanced Wireless Settings (Continued)

Output Power	Select the available transmit power of the access point. This option sets the transmit signal strength of the access point. Increasing the power improves performance, but if two or more access points are operating in the same area, on the same channel, it can cause interference.
RTS Threshold (0-2347)	The transmission mechanism (CSMA/CA or CSMA/CD) for the packets. If the packet size is equal to or less than this threshold, then the data frame is transmitted immediately. However, if the packet size is larger than the specified value, then the transmitting station must send out an Request to Send Threshold (RTS) packet to the receiving station, and then must wait for the receiving station to send back a Clear to Send (CTS) packet before sending the actual packet data.
Fragmentation Length (256-2346)	The maximum packet size that used for fragmentation of data packets. Packets larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation length must be an even number.
Beacon Interval (100-1000)	The time interval for each beacon transmission that allows the access point to synchronize the wireless network.
Aggregation Length (1024-65535, 11n only)	The length that defines the maximum length of Aggregated MAC Protocol Data Unit (AMPDU) packets. Larger aggregation lengths might sometimes lead to better network performance. Aggregation is a mechanism used to achieve higher throughput.
AMPDU (11n only)	Allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling AMPDU can sometimes lead to better network performance.
RIFS Transmission (11n only)	Enable the Reduced Interframe Space (RIFS) option to allow transmission of successive frames at different transmit powers. Enabling RIFS can lead to better network performance.
Enable Wi-Fi MultiMedia (WMM)	Select this check box to ensure that applications that require better throughput and performance are provided special queues with higher priority. For more information about WMM, see *QoS for Managed Access Points* on page 21.
DTIM Interval (1–255)	Enter the DTIM or the data beacon rate that you want to use. This sets the message period of the beacon delivery traffic indication in multiples of beacon intervals.
Preamble Type (11b/bg only)	A long transmit preamble can provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The **Auto** setting automatically handles both long and short preambles. The default is Auto.
Access Point Channel	Each managed access point's channel and frequency can be individually selected. The access point mode is set either to the one enabled for the group, or if the selected mode is not available on the access point, to the mode providing highest performance.

Configuring QoS

You can use QoS to enable WMM for both upstream traffic from the station to the access point and downstream traffic from the access point to the client station.You can use basic QoS settings for access points or advanced QoS settings for access point groups. These settings are applied only to NETGEAR ProSafe access points that support QoS.

WMM defines the following four queues in decreasing order of priority:

- **Voice**: The highest-priority queue with minimum delay, which makes it ideal for applications like VOIP and streaming media.
- **Video**: The second-highest priority with low delay is given to this queue. Video applications are routed to this queue.
- **Best Effort**: The medium priority with medium delay is given to this queue. Most standard IP applications use this queue.
- **Background**: Low-priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue.

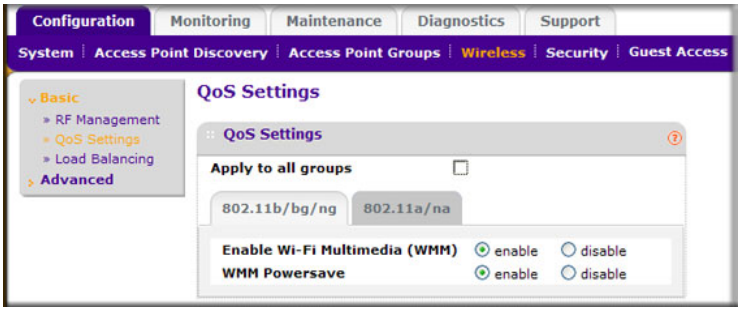
With WMM enabled, QoS prioritizes and coordinates wireless access. QoS settings on the access point control downstream traffic to client stations (AP EDCA parameters) and the upstream traffic from the station to the access point (station EDCA parameters).

Disabling WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point. With WMM disabled, you can still set some parameters on the downstream traffic from the access point to the client stations (AP EDCA parameters).

QoS for Managed Access Points

To specify QoS settings:

1. On the Configuration tab select Wireless > Basic > QoS Settings:



2. Select the **Apply to all groups** check box to apply the settings to all managed access points.
3. Select either the 802.11b/bg/ng or 802.11a/na tab.
4. Enable the **Wi-Fi MultiMedia (WMM)** and **WMM Powersave** options.

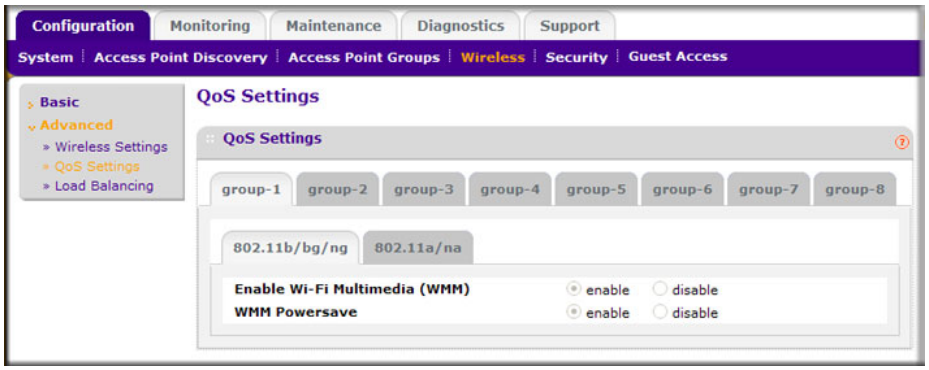
5. Click **Apply**.

Advanced QoS Settings for Access Point Groups

Most QoS settings can be controlled from the Basic QoS Settings screen. If you use access point groups and want to use different QoS settings for specific groups, use the Advanced QoS Settings screen.

To specify advanced QoS settings:

1. On the Configuration tab, select Wireless > Advanced > QoS Settings:



2. Click a tab to select an access point group.
3. Select either the 802.11b/bg/ng or 802.11a/na tab.
4. Enable the **Wi-Fi MultiMedia (WMM)** and **WMM Powersave** options.
5. Click **Apply**.

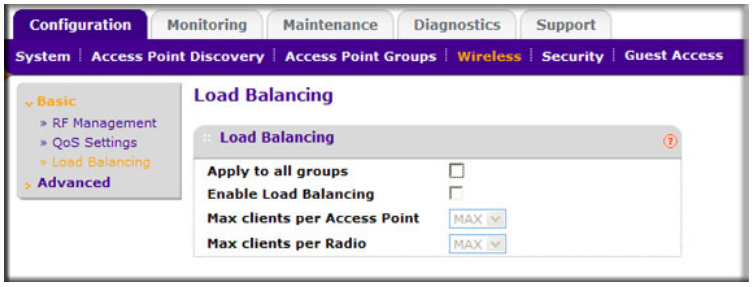
Load Balancing

Load balancing allows the wireless management system to distribute access point clients equally among access points. These settings are applied only to managed NETGEAR ProSafe access points that support load balancing. See *Controller Features and Access Point Compatibility* on page 59 for more information about which access points models support this feature.

You can set up basic load balancing for managed access points or advanced load balancing for access point groups.

Load Balancing for Managed Access Points

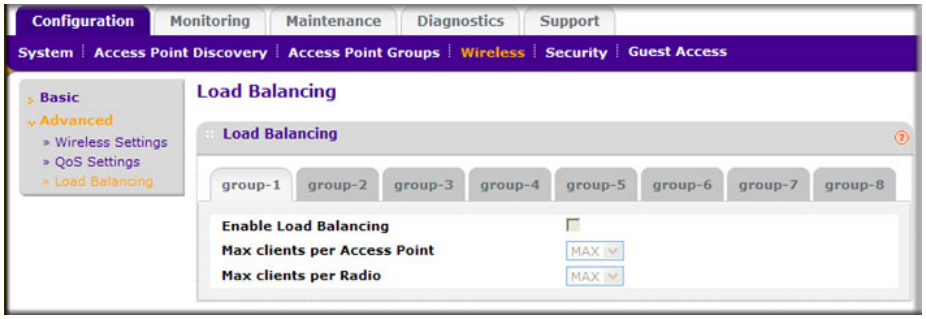
On the Configuration tab select Wireless > Basic > Load Balancing.



- **Apply to all groups**: Select this check box to apply the settings to all managed access points regardless of group.
- **Enable Load Balancing**: Select this check box to allow the wireless management system to distribute access point clients equally among access points.
- **Max Clients per Access Point:** The maximum number of wireless clients that can connect to an access point at one time. You can select **MAX** to allow the maximum supported by the access point.
- **Max Clients per Radio**: The maximum number of wireless clients that can connect to each radio of the access point at one time. You can select **MAX** to allow the maximum supported by the access point.

Advanced Load Balancing for Access Point Groups

On the Configuration tab select Wireless > Advanced > Load Balancing:



- **Enable Load Balancing**: Select this check box to allow the wireless management system to distribute access point clients equally among access points.
- **Max Clients per Access Point:** The maximum number of wireless clients that can connect to the access point at one time. You can select **MAX** to allow the maximum supported by the access point.
- **Max Clients per Radio**: The maximum number of wireless clients that can connect to each radio of the access point at one time. You can select **MAX** to allow the maximum supported by the access point.

Security Configuration

4

Security Profiles Lists

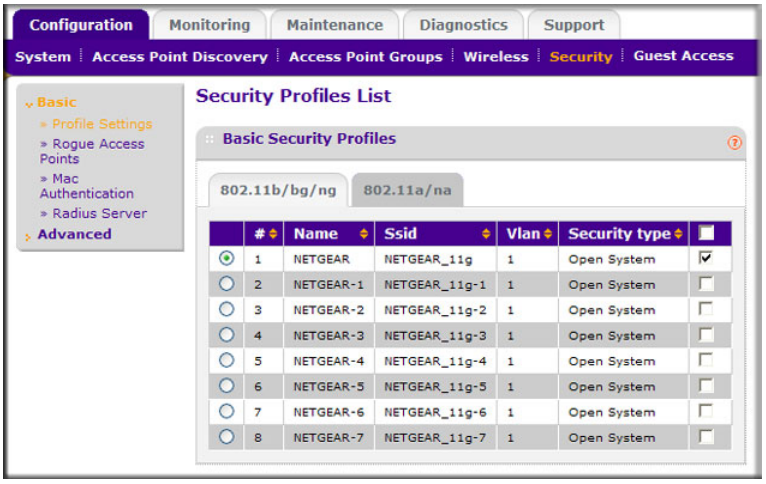
Details of each wireless network are contained in a security profile. You can use the basic profile settings for access points, or the advanced profile settings for access point groups.

Security Profiles List for Access Points

This screen lets you edit up to eight security profiles per managed access point, depending on the number of profiles each access point supports. Separate profiles are applied to 802.11 b/bg/ng and 802.11a/na mode radios.

To view or change security profiles:

1. On the Configuration tab, select Security > Basic > Profile Settings.



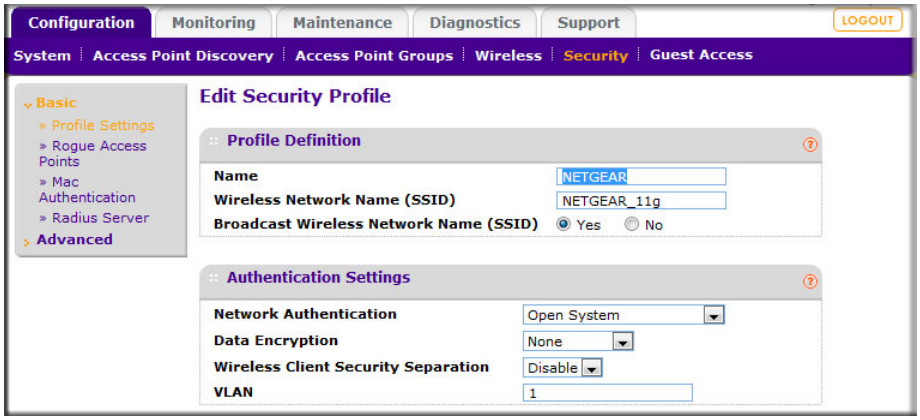
2. Each security profile specifies:
   - **Name**: The unique profile name, up to 31 alphanumeric characters.
   - **SSID**: The SSID associated with this profile.
   - **VLAN**: The VLAN ID associated with this security profile.

- **Security**: The security standard, such as WPA-PSK, associated with the profile.

3. Select the check box to enable (or disable) the corresponding profile.
4. To change the settings of a security profile, select its radio button and click the **Edit** button.

Editing a Security Profile

To edit a security profile, select it on the Profile Settings screen, and then click **Edit** to go to the Edit Security Profile screen:



- **Name**: A unique name for the security profile, up to 32 alphanumeric characters. Use meaningful names instead of the default names. The default profile names are Profile1, Profile2, and so on.
- **Wireless Network Name (SSID)**: The name of the wireless network associated with this profile.
- **Broadcast Wireless Network Name (SSID)**: Enabled by default. If set to **Yes**, the SSID is broadcast. If you disable broadcast of the SSID, only devices that have the correct SSID can connect to the access point.
- **Network Authentication**: The authentication type to be used. See Table 2 on page 26.
- **Data Encryption**: The data encryption type to be used. The options available for data encryption depend on the network authentication settings. See Table 2 on page 26.
- **Wireless Client Security Separation**: If enabled, the associated wireless clients will not be able to communicate with each other. This feature is intended for hot spots and other public access situations.
- **VLAN**: The default VLAN ID to be associated with this security profile. This must match the VLAN ID used by other network devices.

The following table shows the data encryption options based on network authentication.

Table 2. Network Authentication and Data Encryption

Network Authentication	Data Encryption	Description
Open	None. WEP.	No encryption.
Shared Key	WEP.	• 64-bit WEP encryption uses 40/64 bit encryption. • 128-bit WEP encryption uses 104/128 bit encryption. • 152-bit WEP is a proprietary mode that works only with other wireless devices that support this mode.
Legacy 802.1x WPA with RADIUS WPA2 with RADIUS	• Select the WPA2 option only if all clients support WPA2. If this option is selected, you must use AES. • WPA/WPA2 with RADIUS allows clients to use either WPA (with TKIP) or WPA2 (with AES). If this option is selected, you must use TKIP + AES encryption.	All require RADIUS configuration.
WPA-PSK WPA2-PSK	TKIP or TKIP + AES and a WPA passphrase (network key).	Standard encryption method for WPA2.
WPA2-PSK	AES and TKIP + AES .	Some clients support AES with WPA, but this is not supported by this access point.
WPA and WPA2	TKIP + AES encryption and enter the WPA passphrase (network key).	Clients can use either WPA (with TKIP) or WPA2 (with AES).
WPA-PSK/WPA2-PSK:	TKIP + AE.	Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

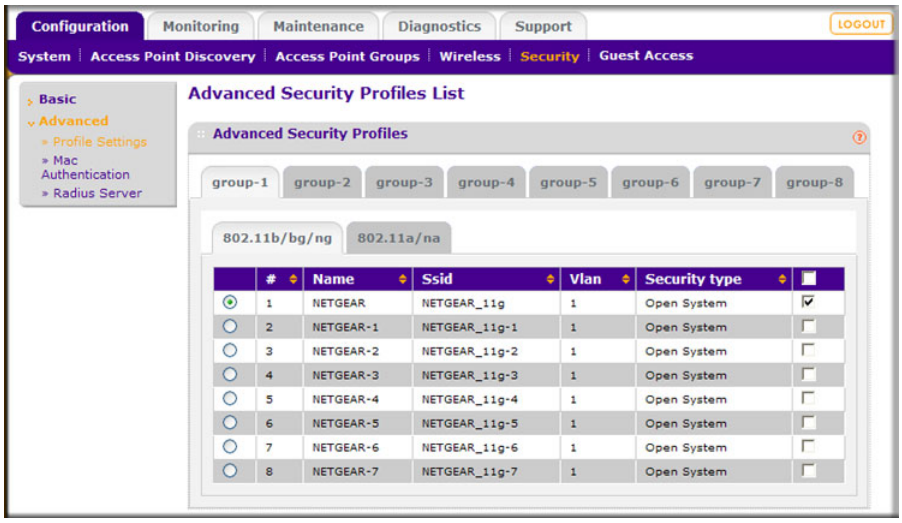
Advanced Security Profiles List for Access Point Groups

Note: Most networks do not require access point groups. See Chapter 1, *Getting Started* for more information about basic settings for a typical network and advanced settings for access point groups.

This screen lets you edit up to eight security profiles for managed access points in the selected group. The number of security profiles applied to managed access point depends on the supported profiles per access point. Separate profiles are applied to 802.11b/bg/ng and 802.11a/na mode radios.

To view or change security profiles for a specific access point group:

1. On the Configuration tab select Security > Advanced > Profile Settings:



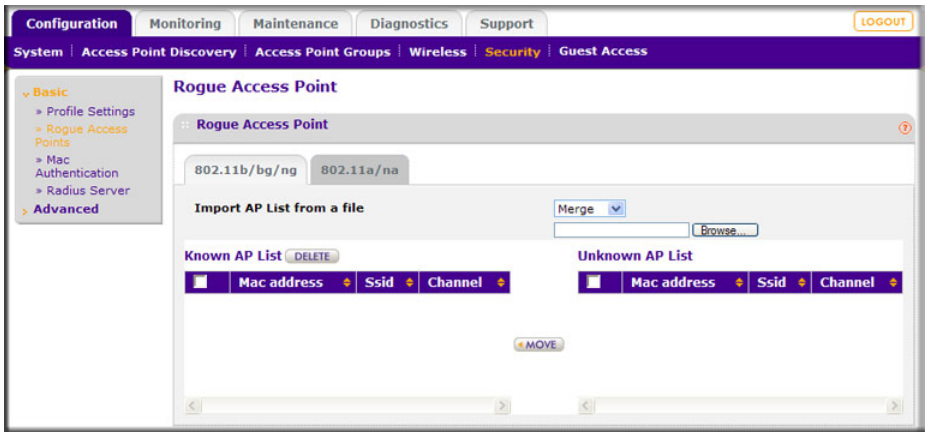
2. Each security profile specifies:
   - **Profile Name**: The unique profile name. This value can be up to 31 alphanumeric characters.
   - **SSID**: The SSID associated with this profile.
   - **Security**: The security standard, such as WPA-PSK, associated with the profile.
   - **VLAN**: The VLAN ID associated with this security profile.
3. Select the a check box to enable the corresponding profile, or clear the check box to disable it.
4. To change the settings of a security profile, select it's radio button and click the **Edit** button. See *Editing a Security Profile* on page 25.

Rogue Access Points

Unidentified access points that use the SSID of a legitimate network can present a serious security threat. Rogue Access Point Detection is enabled by default on managed access points. To detect rogue access points, the wireless management system or access point scans the wireless environment on all available channels, looking for unidentified access points.

To detect rogue access points:

1. On the Configuration tab select Security > Basic > Rogue Access Points:



   The wireless management system can support up to 512 total rogue access points from the Known and Unknown lists combined.

2. Enter the following information:
   - **Import AP List from a file**: This field allows you to import a list of approved access points from a saved file. This file must be a simple text file with one MAC address per line.
   - **Merge**: The current list is maintained, and the access points in the imported list will be added to the approved list and the Known AP List.
   - **Known AP List**: Approved access points. To remove an access point from this list, select its check box and click **Delete**.
   - **Unknown AP List**: Detected unidentified access points.
3. Adjust the Known AP List.
   - You can click **Refresh** to scan for other access points in the vicinity whose details are not in the Known AP List. If such access points are found, they are added to this list.
   - To move an access point from the Unknown AP list to the Known AP list, select its check box and click **Move**.
4. When you are finished making changes, click **Apply**.

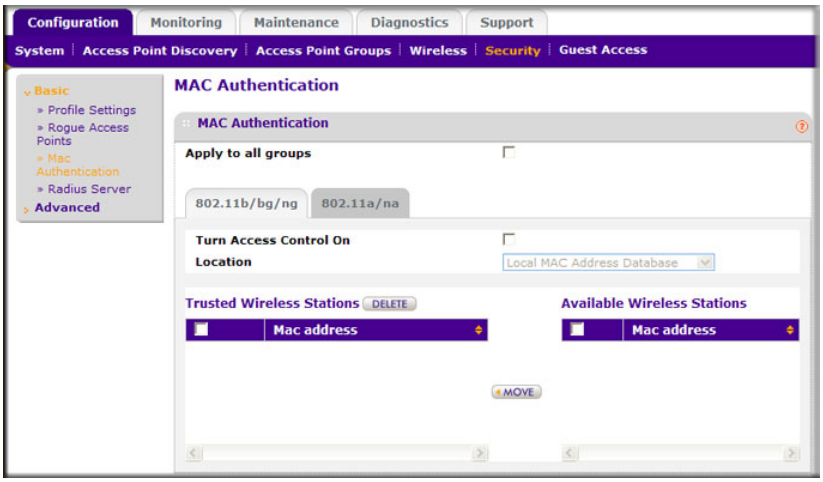
MAC Authentication

This lets you block the network access privilege of the specified stations with the wireless management system–managed access point. The settings are applied only to managed NETGEAR ProSafe access points.

MAC Authentication for Access Points

To set up MAC authentication:

1. On the Configuration tab, select Security > Basic > MAC Authentication:



   A maxiumum of 512 MAC addresses can be supported.

2. Select the **Apply to all groups** check box to apply the settings to all managed access points regardless of group.
3. Select the **Turn Access Control On** check box if you want the access point to interact only with stations present in the Trusted Wireless Stations list. This provides an additional layer of security.
4. Select one of the following databases:
   - **Local MAC Address Database**: The access point will use the local MAC address table for access control.
   - **Remote MAC Address Database**: The access point will use the MAC address table on an external RADIUS server on the LAN for access control.
5. Make sure that the correct wireless stations are in the Trusted Wireless Stations list. If you are using access control, only these stations will be allowed access to the network through this access point.
   - To remove a wireless station from this table, select it and click **Delete**.
   - To add a wireless station to this tablet, enter its MAC address and click **Add**.
   - To move a wireless station from the Available Wireless Stations list to the Trusted Wireless Stations list, select it, and click **Move**.
6. Click **Apply** so that your changes take effect.

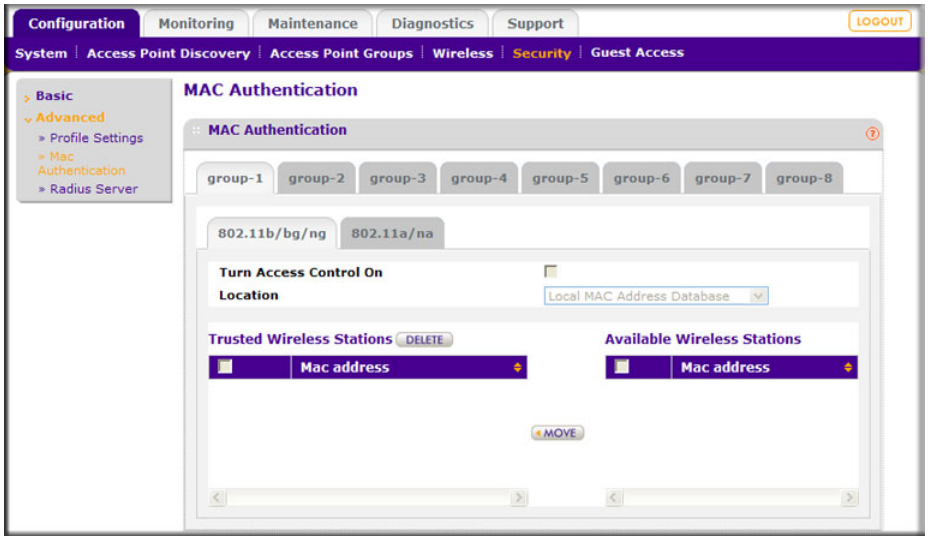
Advanced MAC Authentication for Access Point Groups

This lets you block network access privilege of the specified stations through a specific group of managed wireless access points.

Note: Most networks do not require access point groups. See Chapter 1, *Getting Started* for more information about basic settings and advanced settings for access point groups.

To set up MAC authentication for only the selected access point group:

1. On the Configuration tab, select Security >Advanced > MAC Authentication:.



2. Click a group tab to select the access point group that will use access control.
3. Select the **Turn Access Control On** check box if you want the access point to interact only with stations present in the Trusted Wireless Stations list. This provides an additional layer of security.
4. Select one of the following databases:
   - **Local MAC Address Database**: The access point will use the local MAC address table for Access Control.
   - **Remote MAC Address Database**: The access point will use the MAC address table located on an external RADIUS server on the LAN for access control.
5. Make sure that the correct wireless stations are in the Trusted Wireless Stations list. If you are using access control, only these stations will be allowed access to the network through this access point.
   - To remove a wireless station from this table, select it and click **Delete**.
   - To add a wireless station to this table, enter its MAC address and click **Add**.
   - To move a wireless station from the Available Wireless Stations list to the Trusted Wireless Stations list, select it, and click **Move**.
6. Click **Apply** so that your changes take effect.

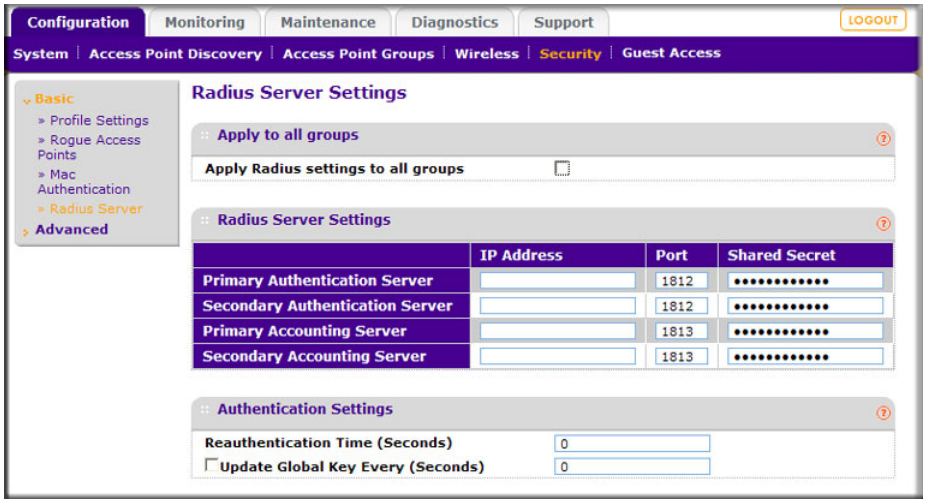
Radius Server Settings

If you are using a RADIUS server in your network for authentication, you must configure Radius settings. You can configure four types of servers:

- **Primary Authentication Server:** The primary authentication server is the main RADIUS server used for authentication.
- **Secondary Authentication Server**: A secondary authentication server can be configured for use if the primary authentication server fails or is unreachable.
- **Primary Accounting Server**: The primary accounting server is used for accounting on the network.
- **Secondary Accounting Server**: A secondary accounting server can be configured for use if the primary authentication server fails or is unreachable.

To configure Radius server settings:

1. Click the Configuration tab and select Security > Basic > Radius Server:



   The primary server is used by default. If the primary server fails, the secondary server is used, if configured.

2. Select **Apply to all groups** to apply the settings to all managed access points regardless of group.
3. Fill in the **IP Address**, **Port**, and **Shared Secret** fields for each RADIUS server.
   - The IP Address, Port, and Shared Secret information is required to communicate with the RADIUS server.
   - The shared secret is shared between the wireless access point and the RADIUS server while the server is authenticating the wireless client.

4. Enter the authentication settings.
   - **Re-authentication Time (Seconds)**: This is the time interval in seconds after which the supplicant will be authenticated again with the RADIUS server. The default interval is 3600 seconds.
   - **Update Global Key Every (Seconds)**: Enable this option to have the global key changed according to the time interval specified. If enabled, enter the time interval you want to use. This option is enabled by default. The default interval is 1800 seconds.
5. Click **Apply** so that your changes take effect.

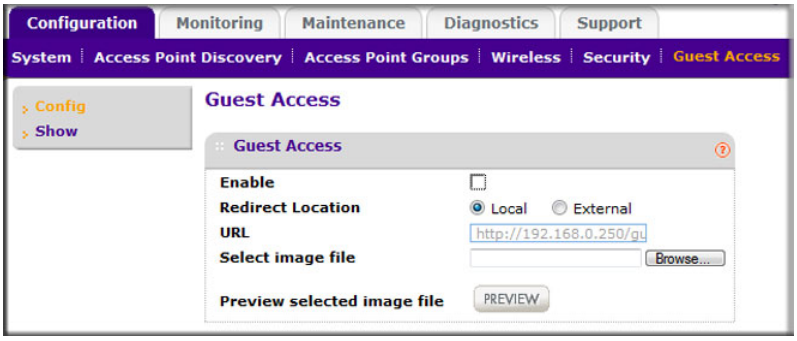
Configuring Guest Access

Guest access settings are useful when you are configuring a public access point. The guest access feature is not a captive portal. You can use guest access to:

- Redirect the user to a guest portal that you specify.
- Allow users to enter simple information such as an email address.
- Identify sessions and track usage.

To set up guest access:

1. On the Configuration tab, select Guest Access > Config:



2. Specify the following settings:
   - **Enable**: Select this check box if you want all HTTP (TCP, port 80) requests to be routed to the URL you specify in the next field.
   - **Redirect Location**: Select **Local** to redirect to a redirect screen on the WMS5316. You can select **External** and enter a URL for redirecting all HTTP (TCP, port 80) requests.
   - **URL**: Enter the URL of the Web server that you want all HTTP requests to be redirected to.
   - **Select Image File**: Specify a jpeg or gif image to upload to the wireless management system. This image is set as background for the default wireless management system redirection screen, which is displayed when a client connects to an access point with guest access enabled.

- **Preview**: Click this button to display how the redirection screen will look.

3. Click **Apply** so that your changes take effect.

Guest Access Show

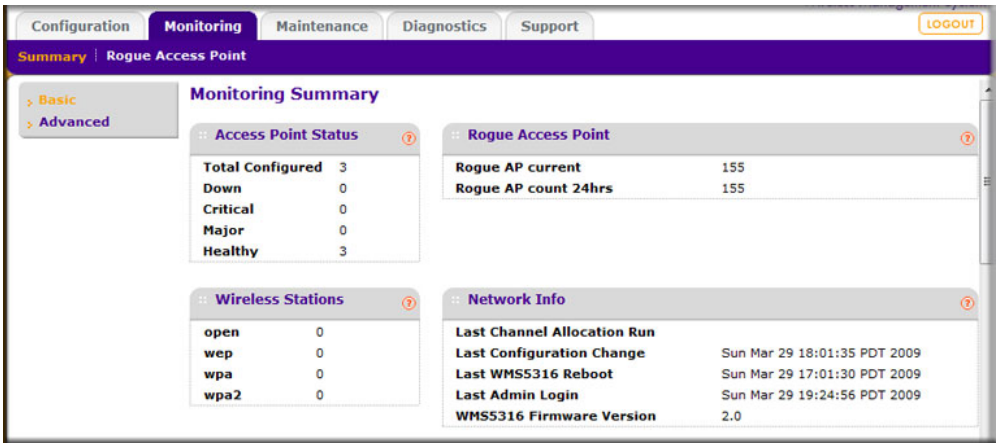
When guest access is configured, the wireless management system redirects the first HTTP (TCP, port 80) request to the default guest access screen. The last 512 IP accesses and entered email address are recorded. This screen displays the collected information.

Monitoring

5

Monitoring Summary

This screen displays a read-only summary of the current managed access point status, rogue access points detected, current wireless stations connected, wireless management system information, and network usage. Clicking the individual sections leads to a new screen showing greater detail.



Access Point Status

This section displays status of managed access points.

- **Total Configured**: Total number of managed access points.
- **Down**: Number of managed access points that cannot be pinged.
- **Critical**: The wireless management system can ping these managed access points, but either cannot log in or has detected that the device is different from the one that was configured.
- **Major**: Number of managed access points whose configuration differs from the one that is set on the wireless management system. This is most likely due to an access point running old firmware or because the wireless management system changed the configuration when the access point was down or offline.

- **Healthy**: Managed access points are running correctly.

Rogue Access Points

This section displays the count of rogue or neighboring access points discovered by managed access points.

- **Rogue AP current**: The number of unique rogue or neighboring access point BSSID that can be observed now.
- **Rogue AP count 24hrs**: The number of unique rogue or neighboring access point BSSID observed over the last 24 hours.

Wireless Stations

This section displays the count of the wireless stations currently associated with managed access points.

- **open**: Wireless stations connected to managed access points using security profiles configured with open mode.
- **wep**: Wireless stations connected to managed access points using security profiles configured with WEP.
- **wpa**: Wireless stations connected to managed access points using security profiles configured with WPA security.
- **wpa2**: Wireless stations connected to managed access points using security profiles configured with WPA2 security.

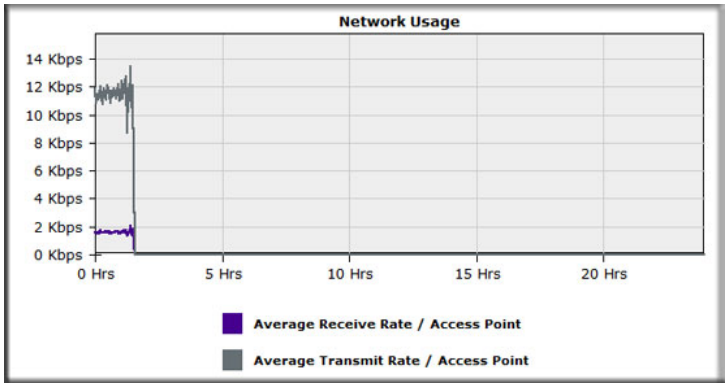
Network Info

This section displays wireless management system information.

- **Last Channel Allocation Run**: When the last automatic channel allocation was performed.
- **Last Configuration Change**: When the configuration changed most recently on the wireless management system.
- **Last WMS5316 Reboot**: The last time the wireless management system was rebooted.
- **Last Admin Login**: The last time the admin user logged in.
- **WMS5316 Firmware version**: The current firmware version running on the wireless management system.

Network Usage

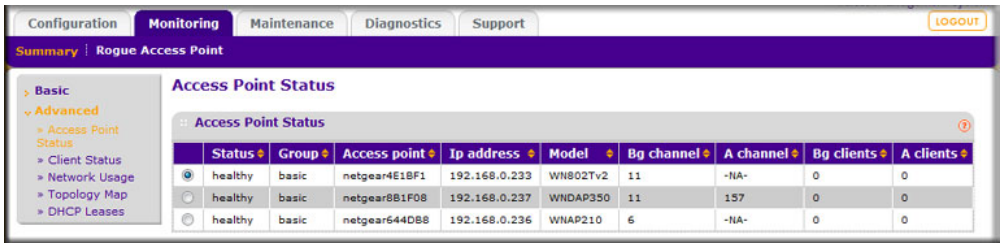
You can scroll down to view network usage:



This section displays a graph of the average data traffic received and transmitted per managed access point over the last 24 hours.

Access Point Status

On the Monitoring tab select Summary > Advanced > Access Point Status:



The access point status screen displays a read-only status summary of managed access points. Each access point entry specifies:

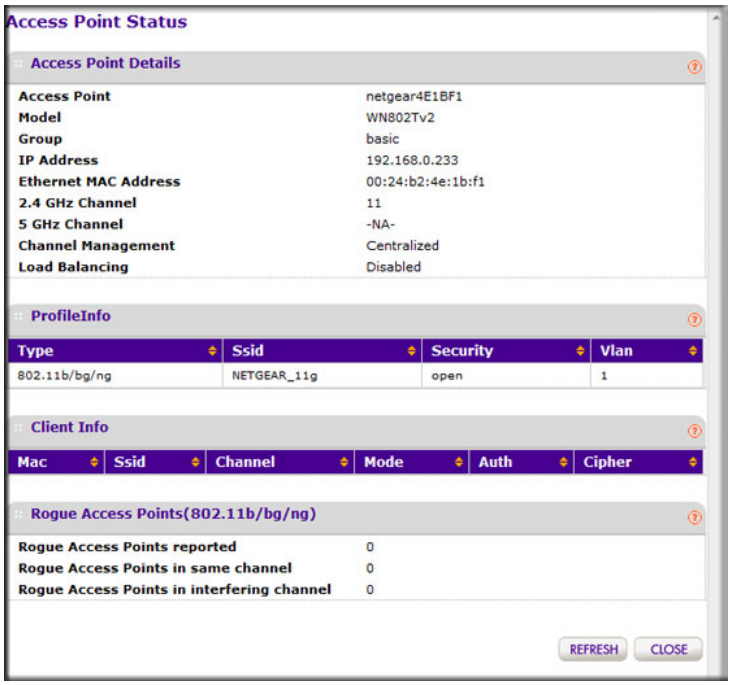
- **Status**: Access point connection and configuration status.
- **Group**: Group configured for the access point. Group 1 is the default setting for unassigned access points.
- **Access Point**: NetBIOS name of the access point.
- **IP address**: Management IP address used by the wireless management system to connect to the access point.
- **Model**: The access point model.
- **B/G channel**: The b/g/n mode channel configured on the access point.
- **A channel**: The a/n mode channel configured for the access point.
- **B/G clients**: The number of client stations connected to the access point using the 2.4 GHz channel.

- **A clients**: The number of client stations connected to the access point using the 5 GHz channel.

Click **Refresh** to update the displayed status of access points. Click **Details** to display detailed status of specific managed access points.

Access Point Status Details

From the Access Point Status screen, click the **Details** button to display this screen:



Click the **Refresh** button to update access point statistics and information.

The Access Point Status screen displays details of an access point that includes configuration settings, current wireless settings, current clients, and current traffic statistics.

- **Access Point Name**: The access point's NetBIOS name.
- **Model**: The managed access point's model.
- **Group**: The configured group of the managed access point.
- **IP Address**: The IP address of the managed access point.
- **Ethernet MAC Address**: The Ethernet MAC address of the managed access point.
- **2.4 GHz Channel**: 2.4 GHz channel configured on the access point; set to -NA- if not available.
- **5 GHz Channel**: 5 GHz channel configured on the access point; set to -NA- if not available.
- **Load Balancing**: The enabled or disabled status of the access point.

Profile Information

The section displays configured and enabled security profiles on the access point.

- **Type**: 802.11 b/bg/ng or 802.11 a/na mode for the security profile.
- **SSID**: Wireless network name.
- **Security**: The mode of security configured for the profile.
- **VLAN**: VLAN configured for the security profile.

Client Information

This section displays client station information for the access point.

- **MAC**: Wireless MAC address of the access point client.
- **SSID**: Wireless SSID configured on the managed access point to which the client connects.
- **Channel**: The channel that the client is using to connect.
- **Mode**: The mode (802.11 b/bg/ng or 802.11 a/na) for the security profile.
- **Auth**: The security authentication mode (open, WEP, WPA, or WPA2).

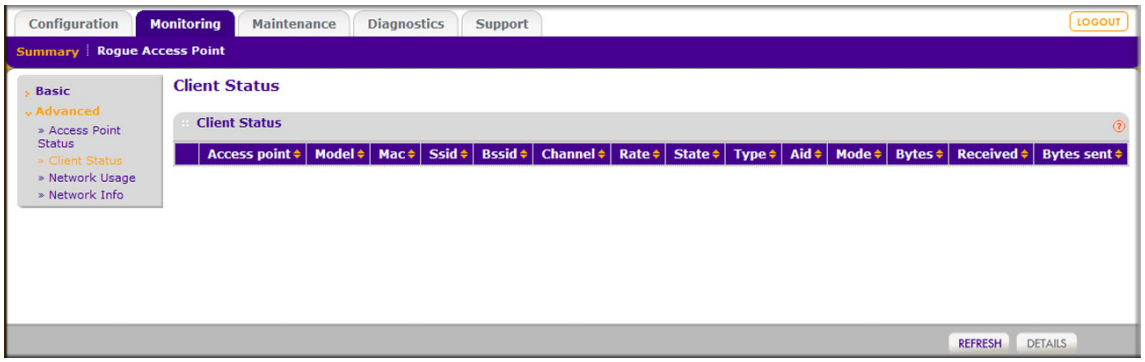
Rogue Access Points

This section displays rogue or neighboring access points detected by the managed access point.

- Rogue Access Points Reported.
- Rogue Access Points in same channel.
- Rogue Access Points in interfering channels.

Client Status

On the Monitoring tab select Summary > Advanced > Client Status:



The Client Status list specifies detailed information about each client node currently associated with managed access points.

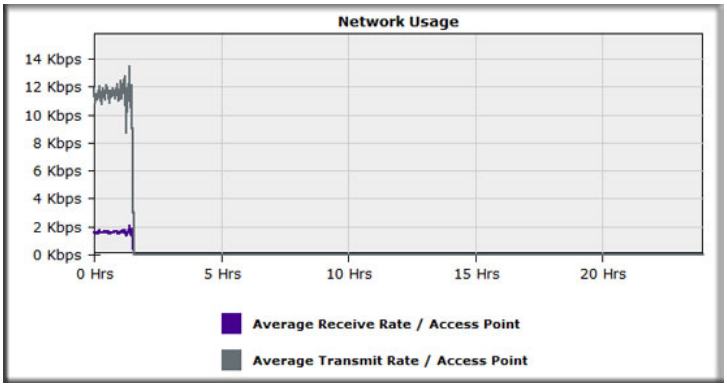
- Click the **Refresh** button to update the list of available wireless stations.
- Click the **Details** button to get details of a selected wireless station.

Network Usage

You can use this screen to view network usage statistics or network topology.

Network Usage Statistics

On the Monitoring tab select Summary > Advanced > Network Usage to display this screen:

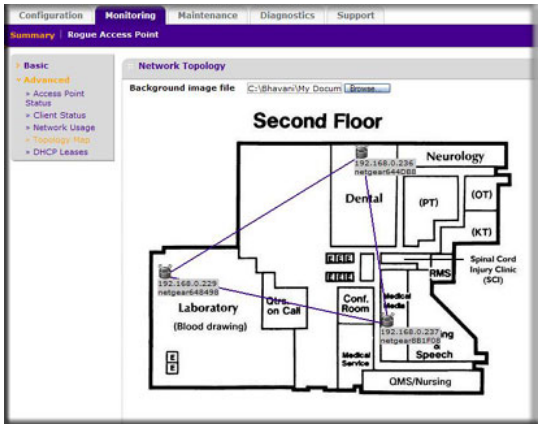


Scroll down to view wireless statistics.

The screen displays plots of average received and transmitted network traffic per managed access point. Three different plots show Ethernet, wireless 802.11 b/bg/ng, and wireless 802.11 a/na mode traffic separately.

Click the **Refresh** button to update the plots.

Network Topology



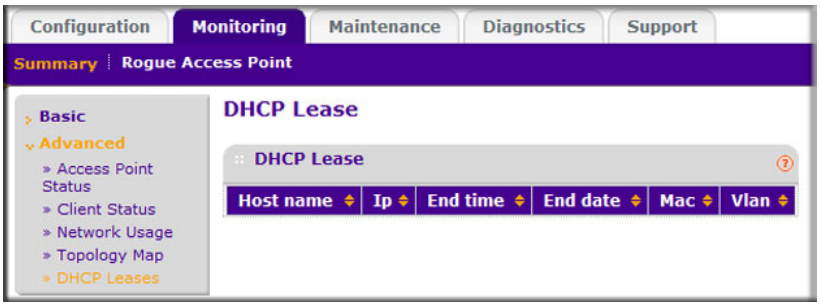
- **Display topology graph of the managed Access Points.** It displays a graph of managed access point connectivity. The access point icons can be moved on the

topology background and their locations saved for later displays.

- **Background Image File**: Specify the image file that you want to use for the floor map. The image should be 800 x 600 in size and can be in either jpg or gif format. When the image is uploaded it is displayed as the topology background.
- Click the **Refresh** button to update the connectivity status.
- Click the **Apply** button to save the location of the access points on the floor displayed floor map.

DHCP Leases

The DHCP Lease screen displays current DHCP clients that have been allocated IP addresses. On the Monitoring tab select Summary > Advanced > DHCP Leases:



This screen displays information about the DHCP lease provided by DHCP server on the wireless management system.

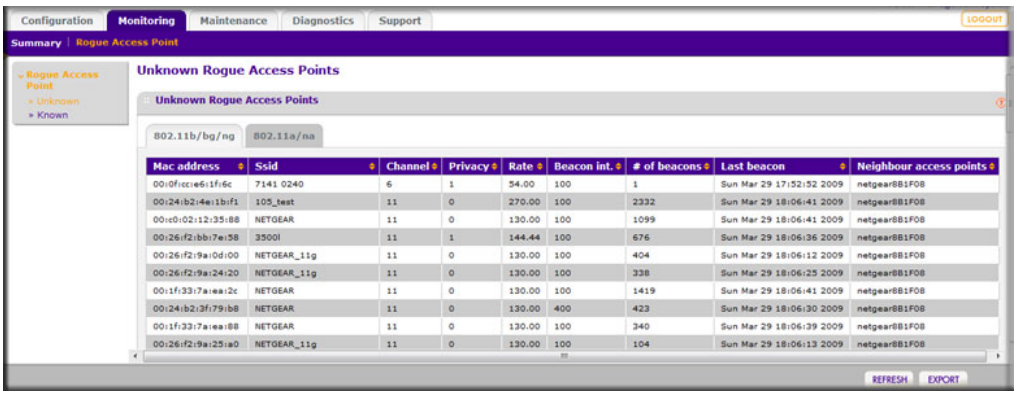
- **Host name**: The host name of the client, if possible to determine.
- **IP**: The IP address allocated to the DHCP client by the wireless management system.
- **End time**: The DHCP lease end time for the DHCP client.
- **End date**: The DHCP lease end date for the DHCP client.
- **MAC**: The Ethernet MAC address of the DHCP client.
- **VLAN**: The VLAN the client is using to connect.

Use the **Refresh** button to update the client DHCP lease display.

Monitoring Rogue Access Points

On the Monitoring tab select Rogue Access Point. You can view rogue or unknown access points.

To display the list of unknown rogue access points, On the Monitoring tab, select Rogue Access Point> Unknown:


Configuration
Monitoring
Maintenance
Diagnostics
Support
LOGOUT
Summary | Rogue Access Point
Rogue Access Point
» Unknown
» Known
Unknown Rogue Access Points
Unknown Rogue Access Points
802.11b/bg/ng
802.11a/na
Mac address
Ssid
Channel
Privacy
Rate
Beacon int.
# of beacons
Last beacon
Neighbour access points
00:0f:cc:e6:1f:6c 7141 0240 6 1 54.00 100 1 Sun Mar 29 17:52:52 2009 netgear8B1F08
00:24:b2:4e:1b:f1 105_test 11 0 270.00 100 2332 Sun Mar 29 18:06:41 2009 netgear8B1F08
00:c0:02:12:35:88 NETGEAR 11 0 130.00 100 1099 Sun Mar 29 18:06:41 2009 netgear8B1F08
00:26:f2:bb:7e:58 3500l 11 1 144.44 100 676 Sun Mar 29 18:06:36 2009 netgear8B1F08
00:26:f2:9a:0d:00 NETGEAR_11g 11 0 130.00 100 404 Sun Mar 29 18:06:12 2009 netgear8B1F08
00:26:f2:9a:24:20 NETGEAR_11g 11 0 130.00 100 338 Sun Mar 29 18:06:25 2009 netgear8B1F08
00:1f:33:7a:ea:2c NETGEAR 11 0 130.00 100 1419 Sun Mar 29 18:06:41 2009 netgear8B1F08
00:24:b2:3f:79:b8 NETGEAR 11 0 130.00 400 423 Sun Mar 29 18:06:30 2009 netgear8B1F08
00:1f:33:7a:ea:88 NETGEAR 11 0 130.00 100 340 Sun Mar 29 18:06:39 2009 netgear8B1F08
00:26:f2:9a:25:a0 NETGEAR_11g 11 0 130.00 100 104 Sun Mar 29 18:06:13 2009 netgear8B1F08
REFRESH
EXPORT

Click **Refresh** to update the access point list, or click **Export** to save the list to a file.

To display the list of known rogue access points, on the Monitoring tab select Rogue Access Point > Known:

Click **Refresh** to update the access point list, or click **Export** to save the list to a file.

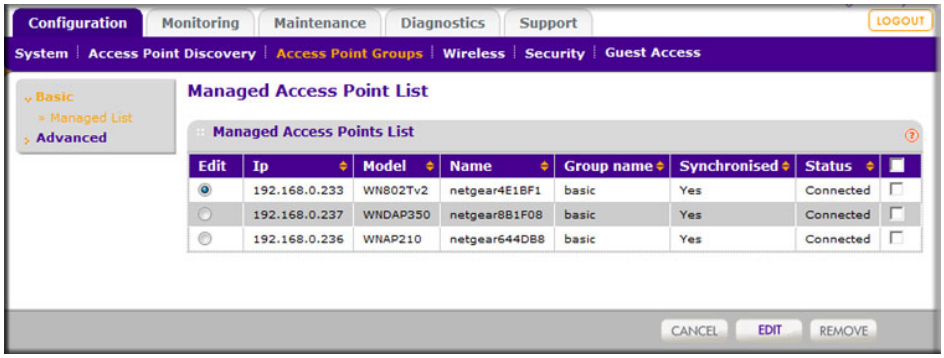
Configuring Access Point Groups

6

Most networks do not need access point groups. Access point groups are useful if completely separate networks share a single LAN. For example, a shopping mall might need access point groups if several businesses share a LAN, but each business has its own network.

Managed Access Point List

On the Configuration tab, select Access Point Groups to display the Managed Access Point List:



This screen shows details of each controlled access point. You can edit the connection settings for specific access points. Each access point entry shows:

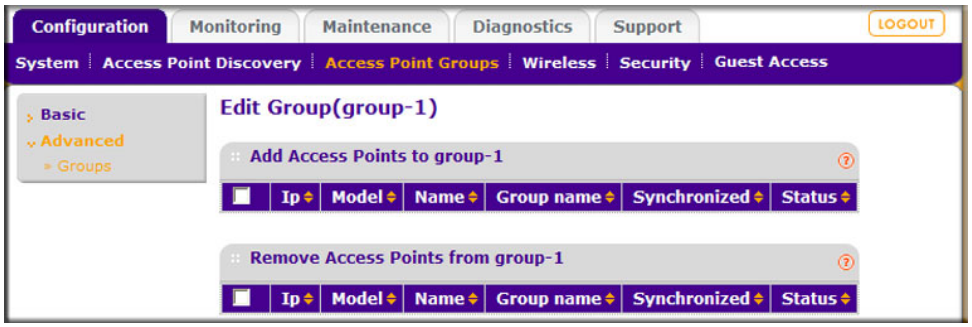
- **IP**: The IP address of the access point.
- **Model**: The access point model.
- **Name**: The name you specify for the access point.
- **Group Name**: The name you specify for the access point group.
- **Synchronized**: Shows whether or not the access point is synchronized with the wireless management system.
- **Status**: The access point connection status.

To change the settings of an access point, select it and click the **Edit** button. You can use the Edit screen for each access point to change its IP settings, VLAN settings, and password.

Table 3. Status Field Definitions

Status	Implies	How to Correct
Connected	Normal operation. The wireless management system is able to contact the access point and manage it.	N/A
Authentication Failure	The password configured during synchronization from the wireless management system is not the same as the password of the access point.	Select the access point and click **Edit**. In the Edit screen, configure the correct password of the access point and click **Apply**. The wireless management system tries again to synchronize with the access point.
Not Connected	The wireless management system cannot connect to the access point with the configured IP address.	The wireless management system tries to log in to managed access points every 1 minute. If the error is temporary, then the status automatically changes to connected. If the error is prolonged, verify the access point IP address and network connection.

Editing Access Point Information



- **IP**: The IP address of the managed access point.
- **Model**: The access point model. The field cannot be modified; it is set when the access point is added to the list.
- **Name**: The user name for logging in to the access point. This field is not modifiable.
- **Password**: The password for the access point. If you use the wireless management system to change a password for an access point, if it is offline or down, its password does not change. When the access point is unauthenticated, the new password is used to authenticate to the access point, and if successful, the new password is saved.
- **Group Name**: You can assign a group name from which the settings will applied to configure the access point.

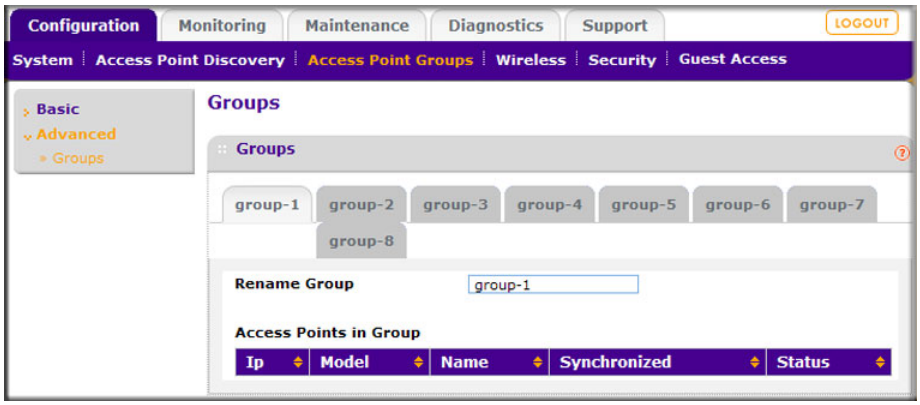
IP Settings

This screen lets you configure the management IP address settings of managed access points.

- **DHCP Client**: Enables the DHCP client on the access point. Do not enable this unless a DHCP server is configured to provide access points the same IP address every time. The WMS5316 will not recognize the access point as the same if its IP address changes.
- **IP Address**: This is the IP address of the managed access point. To change it, enter an unused IP address from the address range used on your LAN. This is allowed only when the access point is online and healthy.
- **Subnet Mask**: Enter the subnet mask value used on your LAN. The default value is 255.255.255.0.
- **Default Gateway**: Enter the IP address of the gateway for your LAN.

Access Point Groups

This screen displays details of each access point in a configured group managed by the wireless management system. You can rename a group and add or delete other managed access points from the group. On the Configuration tab, select Access Point Groups:



- To change group members, click the **Edit** button.
- To add access points to the group, select the access points. They will be synchronized to the settings you specified for the group.
- Click **Apply** so that your changes take effect.

Each access point shows the following information:

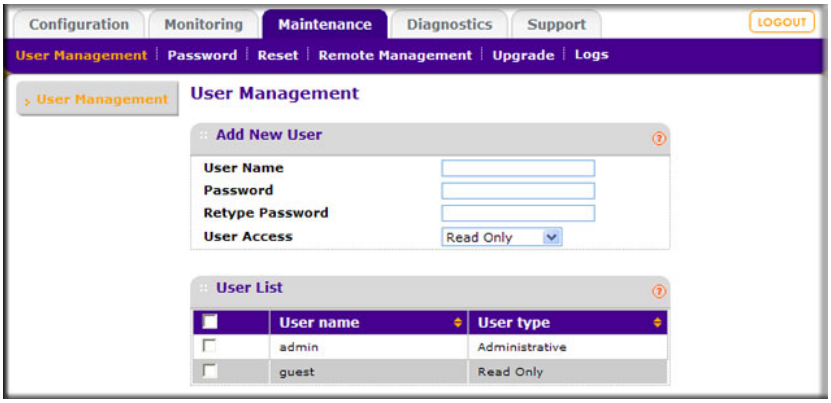
- **IP**: The IP address of the access point.
- **Model**: The access point model.
- **Name**: The name you specify for the access point.
- **Synchronized**: The synchronization status of the access point configuration.
- **Status**: The access point connecton status.

Maintenance

7

User Management

The User Management screen lets you add and remove users. The user name **admin** is the default user name with administrative privileges and cannot be removed. On the Maintenance tab select User Management:

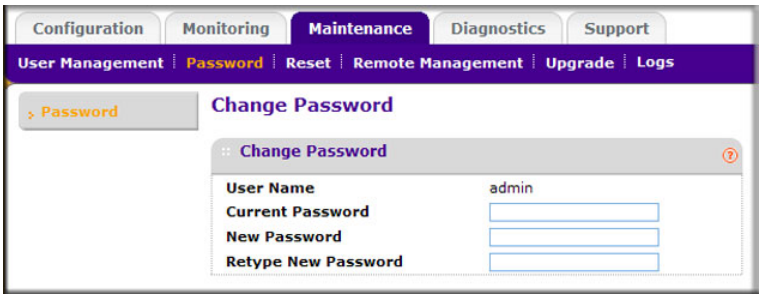


1. Fill in the following fields:
   - **User Name**: Add the name of the user.
   - **Password**: Type a new user password.
   - **Retype Password**: Retype the new user password to confirm.
   - **User Access**: Specify the type of access permitted to the wireless management system user **Read-only** or **Administrative**. A read-only user cannot make any configuration changes. This user is allowed to see the all the statistics and configuration information.
2. Click the **Add** button to add the user information entered. Up to eight users including admin can be added.

To remove users, select their check boxes and click **Remove**.

Changing Passwords

This screen enables you to change the access point administrator's password. On the Maintenance tab, select Password:



To change the password:

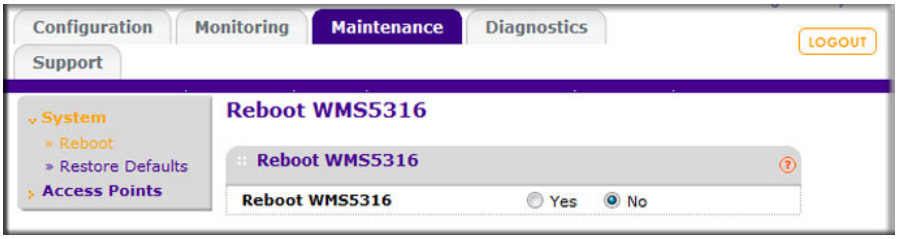
1. Type the old password. (The default password for the user name admin is **password**.)
2. Type a new password, and type it again in the **Repeat New Password** field to confirm it.
3. Be sure to record it in a secure location.
4. Click **Apply** so that your changes take effect, or click **Cancel** to keep the current password.

Reset

The Reset screen lets you reboot the wireless management system, restore factory settings to the wireless management system, or reboot a managed access point.

Rebooting the Wireless Management System

On the Maintenance tab select System > Reboot:

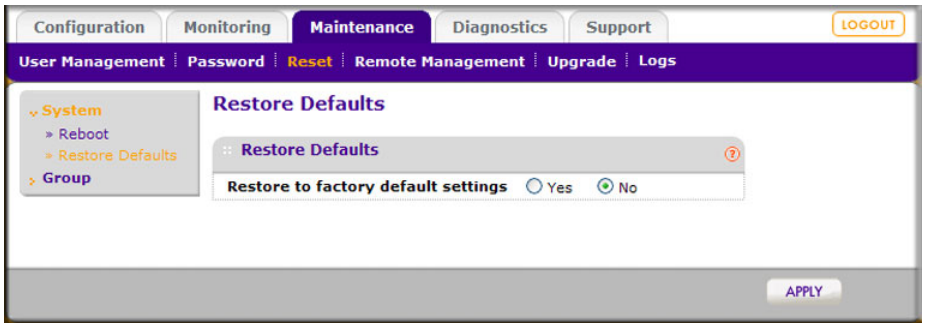


Select the **Yes** radio button, and then click **Apply** to reboot the wireless management system.

Restoring Factory Default Settings

You can restore the factory default settings (listed in Appendix B, *Factory Default Settings*) to the wireless management system.

Note: Restoring the factory default settings of the wireless management system does *not* restore the settings of the access points that are managed by the wireless management system.



To restore the wireless management system settings to factory defaults:

1. Select **Yes**.
2. Click **Apply** to restore factory default settings.

   After restoring factory default settings, the wireless management system restarts. This takes about 1 minute.

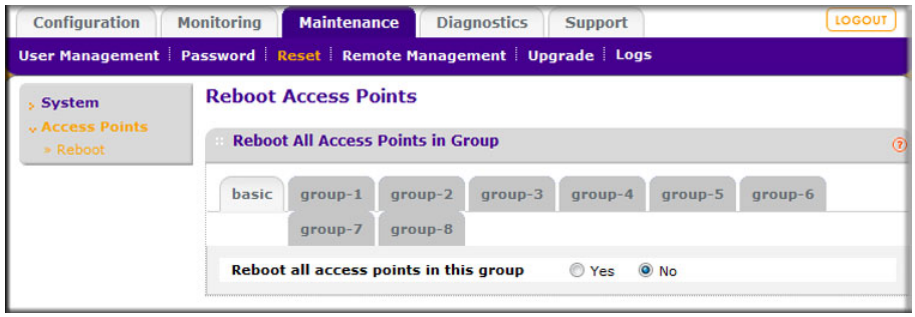
WARNING!

Do not try to go online, turn off the access point, shut down the computer, or do anything else to the wireless management system until it finishes restarting!

When the Test light turns off, wait a few more seconds before doing anything with the wireless management system.

Rebooting an Access Point Group

On the Maintenance tab select Reset > Access Points > Reboot:



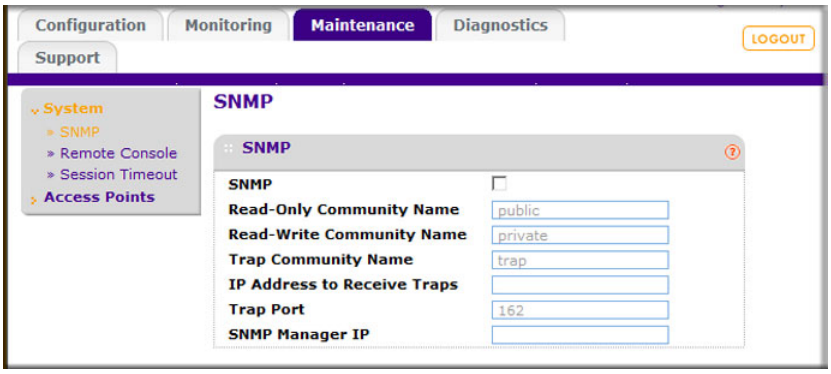
1. Select the group of access points to be rebooted using the tabs. Access points not assigned to a specific group belong to Group 1.
2. Select the **Yes** radio button.
3. Click **Apply** to reboot the access points in the selected group.

SNMP

You can use SNMP for the wireless management system or advanced SNMP for access point groups. Enable SNMP to allow the SNMP network management software, such as HP OpenView, to monitor the wireless management system by using SNMPv1/v2 protocol.

SNMP for the Wireless Management System

On the Maintenance tab, select System > SNMP:



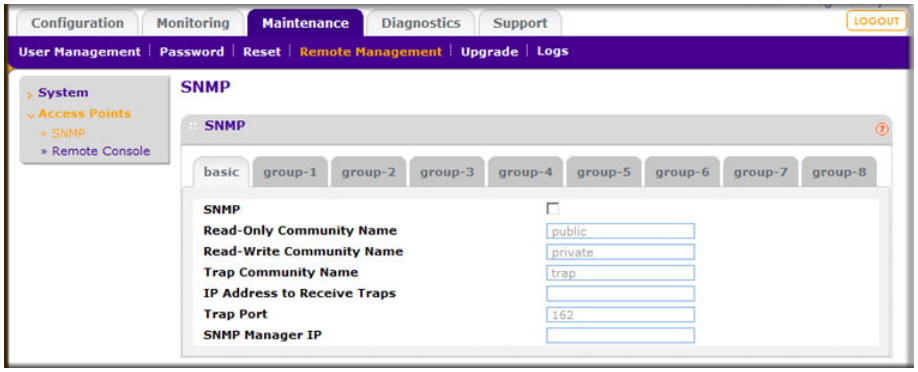
- **SNMP**: Select this check box to enable SNMP for the wireless management system.
- **Read-Only Community Name**: The community string that allows the SNMP manager to read the WMS5316 MIB objects.
- **Read-Write Community Name**: The community string that allows the SNMP manager to read and write the WMS5316 MIB objects.

- **Trap Community Name**: The community name that is associated with the IP address to receive traps.
- **IP address to Receive Traps**: The IP address at which the SNMP manager receives traps sent from the wireless management system.
- **Trap Port**: The port on which the SNMP manager receives traps sent from the wireless management system. The default setting is port 162.
- **SNMP Manager IP**: Restrict access to the specified SNMP manager for doing SNMP v1/v2. Set this to 255.255.255.255 to allow any SNMP manager to access.

When you are finished making changes, click **Apply** to save your settings.

SNMP for Access Point Groups

Enable SNMP to allow the SNMP network management software, such as HP OpenView, to monitor the managed access points by using SNMPv1/v2 protocol. These settings are only applied only on ProSafe access points that support SNMP.



Use the Group tab to select the settings for a specified group of access points. The access points that have not been assigned any group share the settings of Group 1.

- **Read-Only Community Name**: The community string that allows the SNMP manager to read managed wireless access point MIB Objects.
- **Read-Write Community Name**: The community string that allows the SNMP manager to read and write managed wireless access point MIB objects.
- **Trap Community Name**: The community name of the IP address to receive traps.
- **IP Address to Receive Traps**: The IP address at which the SNMP manager receives traps sent from managed wireless access points.
- **Trap Port**: The port on which the SNMP manager receives traps sent from the managed wireless access points. The default setting is port 162.
- **SNMP Manager IP**: Restrict access to specified SNMP manager for doing SNMP v1/v2. Set this to 255.255.255.255 to allow any SNMP manager to access. This setting is specific to WG103 access points, and is not applied to any other access point models.

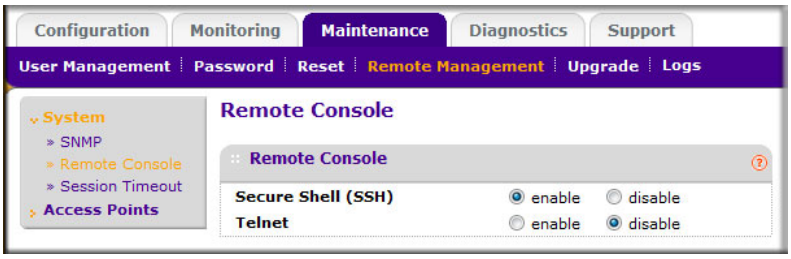
Click **Apply** to save the settings.

Remote Management

You can enable SSH or Telnet in order to remotely log in to the controller or access point groups.

Remote Console for the Wireless Management System

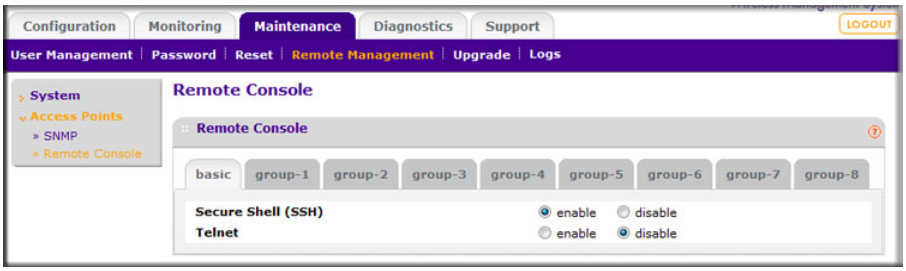
From the Maintenance tab select Remote Management > System > Remote Console:



1. Select the radio button for SSH or Telnet:
   - **Secure Shell (SSH)**: If set to **Enable**, the wireless management system will allow remote access by using Secure Shell.
   - **Telnet**: If set to **Enable**, the wireless management system allows remote access by using Telnet.
2. Click **Apply** to save your settings.

Advanced Remote Console for Access Point Groups

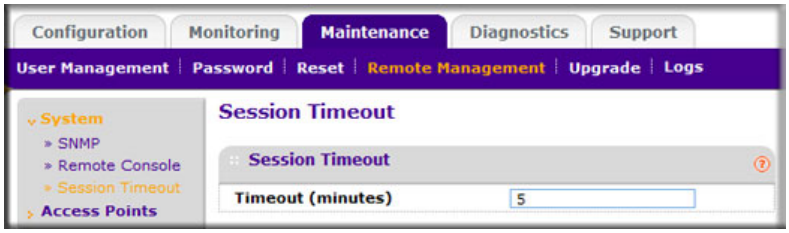
Enable SSH or Telnet to log in to managed access points. These settings are applied only on managed ProSafe access points that support SSH and Telnet.



1. Use the Group tab to select the settings for a specified group of access points. The access points that have not been assigned any group share the settings of Group 1.
   - **Secure Shell (SSH)**: If set to **Enable**, the access points allow remote access using Secure Shell.
   - **Telnet**: If set to **Enable**, the access points allow remote access using Telnet.
2. Click **Apply** to save the selected settings.

Session Timeout

If a session times out, the user is redirected to the login window for password verification.



To specify the length of the session timeout for the wireless management system:

1. In the **Timeout (minutes)** field, specify number of minutes before an active HTTP/HTTPS login session expires.
2. Click **Apply** to save your change.

Upgrading the Firmware

You can use the Firmware Upgrade screen to install newer versions of firmware for the wireless management system or for access points.

Upgrading the Wireless Management System Firmware

WARNING!

In some cases, such as a major upgrade, you might need to erase the configuration and manually reconfigure the wireless management system after upgrading it. See the Release Notes included with the software to find out if you need to reconfigure.

To upgrade the firmware:

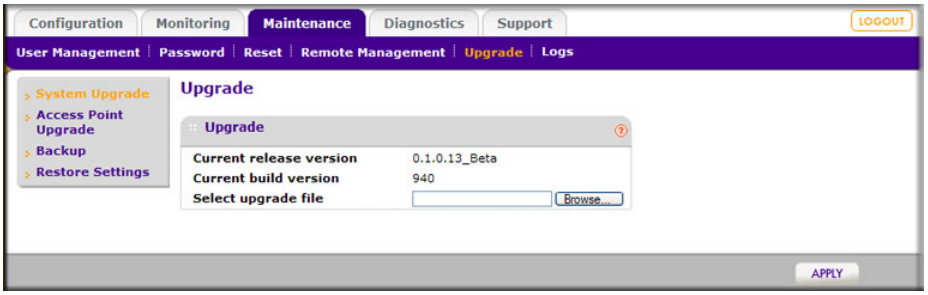
1. Go to the NETGEAR website at *www.netgear.com* customer service downloads section to get new versions of the firmware.

WARNING!

Once you click Upload, do *not* interrupt the process of sending the new firmware to the wireless management system and restarting the unit.

2. Download the new firmware.

3. On the Maintenance tab select Upgrade > System Upgrade:



4. On the Upgrade screen, click **Browse**.
5. Locate and select the file you downloaded.
6. Click **Apply** to send the software to the wireless management system.

   This loads the new software into the wireless management system and causes the wireless management system to restart.

Note: Do not try to go online, turn off the wireless management system, shut down the computer, or do anything else to the wireless management system until it finishes restarting! When the Test light turns off, wait a few more seconds before doing anything.

7. Check the Monitoring screen to see the firmware version to verify that the new software is installed.

Upgrading Access Point Firmware

You can install a new version of the access point's firmware using the Access Point Upgrade screen.

WARNING!

In some cases, such as a major upgrade, you might need to erase the configuration of your access point after upgrading it.

See the Release Notes included with the software to find out if you need to reconfigure the access point. Reconfiguring access points already managed by the wireless management system requires only the IP address to be set manually. The wireless management system restores configuration for already managed access points running the supported firmware version.

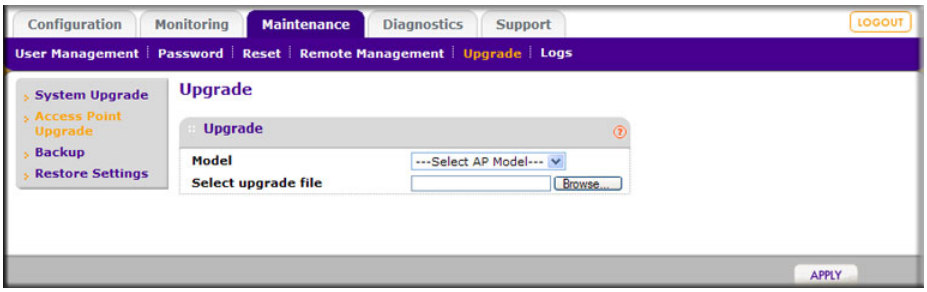
To upgrade the access point software:

1. Go to the NETGEAR website at *www.NETGEAR.com* customer service downloads section to get new versions of the access point software for supported models. After downloading an upgrade file, you might need to unzip (uncompress) it before upgrading the access point.

WARNING!

Once you click Upload, do *not* interrupt the process of sending the software to the access point and restarting the access point.

2. Download the new software for a specific access point model to upgrade.
3. If not done automatically, uncompress the downloaded file. If included, read the Release Notes before continuing.
4. On the Maintenance tab select Upgrade > Access Point Upgrade:



5. Make sure that status of the managed access point to be upgraded is healthy. Select the managed access point model from the drop-down list; only models of managed access points are in this list.
6. Click **Browse**.
7. Locate and select the file you just downloaded.
8. Click **Upload** to send the software to the access point.

   This loads the new software into the access point and causes the access point to restart.

Note: Do not try to go online, turn off the access point, shut down the computer or the wireless management system, or do anything else to the access point or the wireless management system until the access point finishes restarting! When the Test light turns off, wait a few more seconds before doing anything.

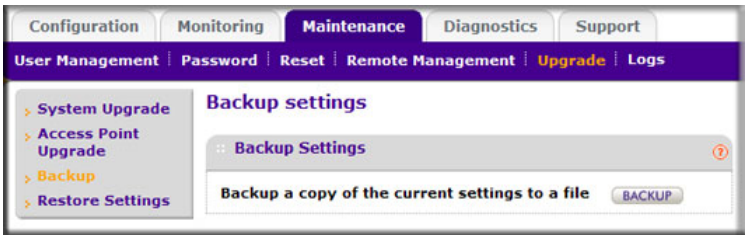
9. Check the firmware version on upgrade screen to verify that your access point now has the new software installed.

Backing Up Configuration Settings

Once you have the wireless management system working correctly, you should back up the information to have it available if something goes wrong. When you back up the settings, they are saved as a file on your computer.

To back up the wireless management system settings:

1. On the Maintenance tab select Upgrade > Backup:



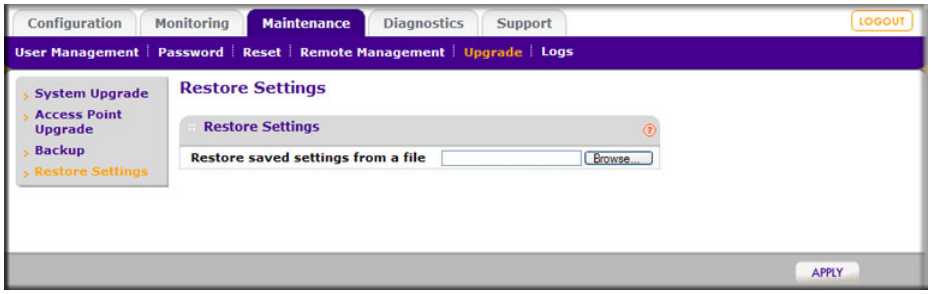
2. Click the **Backup** button to create a backup file of the current settings:
3. If you do not have your browser set up to save downloaded files automatically, then locate where you want to save the file, and rename it if you like.

   If your browser is set up to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.
4. Click **Backup**.

Restoring Settings from a File

To restore settings from a backup file:

1. On the Maintenance tab select Upgrade > Restore Settings:



2. Click **Browse**.
3. Locate and select the previously saved backup file, and click **Apply**.

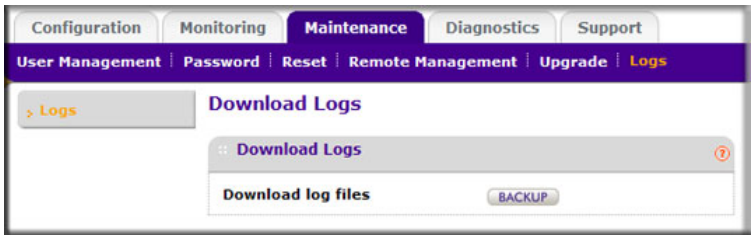
   After restoring previous settings, the wireless management system restarts. This takes about 1 minute.

WARNING!

Do not try to go online, turn off the wireless management system, shut down the computer, or do anything else until it finishes restarting! When the Test light turns off, wait a few more seconds before doing anything with the wireless management system.

Downloading Wireless Management System Logs

You can download logs collected on the wireless management system. In the event of a problem or failure, these logs along with backed up configuration settings help developers determine the cause.



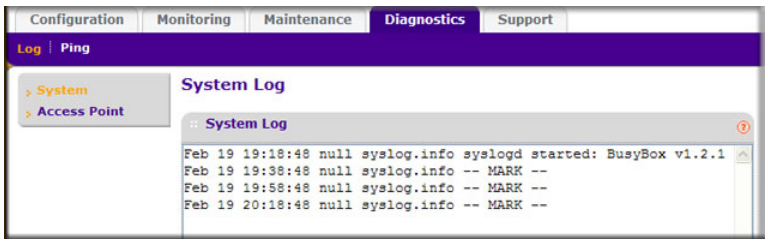
To download logs:

1. On the Maintenance tab, select Logs.
2. Click **Backup** to create a backup file of the current logs.
3. If you do not have your browser set up to save downloaded files automatically, then locate where you want to save the file, and rename it if you like.

   If your browser is set up to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.
4. Click **Backup**.

System Logs

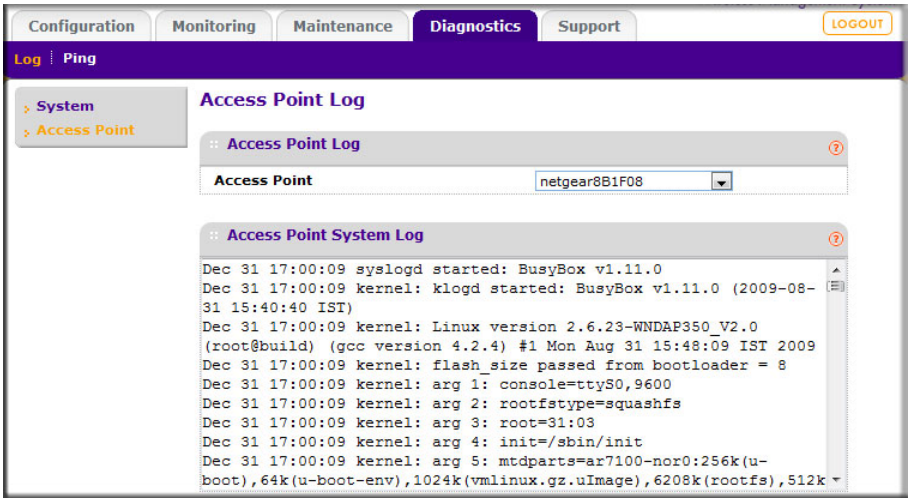
The System Log screen displays wireless management system system activity. On the Diagnostics tab, select System:



You can click **Refresh** to update this screen. To clear the existing log, click **Clear**. Preferably save the contents prior to clearing system log.

Access Point Logs

The Access Points Log screen displays managed access point system activity.


Configuration
Monitoring
Maintenance
Diagnostics
Support
LOGOUT
Log | Ping
System
Access Point
Access Point Log
Access Point Log
Access Point
netgear8B1F08
Access Point System Log
Dec 31 17:00:09 syslogd started: BusyBox v1.11.0
Dec 31 17:00:09 kernel: klogd started: BusyBox v1.11.0 (2009-08-31 15:40:40 IST)
Dec 31 17:00:09 kernel: Linux version 2.6.23-WNDAP350_V2.0 (root@build) (gcc version 4.2.4) #1 Mon Aug 31 15:48:09 IST 2009
Dec 31 17:00:09 kernel: flash_size passed from bootloader = 8
Dec 31 17:00:09 kernel: arg 1: console=ttyS0,9600
Dec 31 17:00:09 kernel: arg 2: rootfstype=squashfs
Dec 31 17:00:09 kernel: arg 3: root=31:03
Dec 31 17:00:09 kernel: arg 4: init=/sbin/init
Dec 31 17:00:09 kernel: arg 5: mtdparts=ar7100-nor0:256k(u-boot),64k(u-boot-env),1024k(vmlinux.gz.uImage),6208k(rootfs),512k

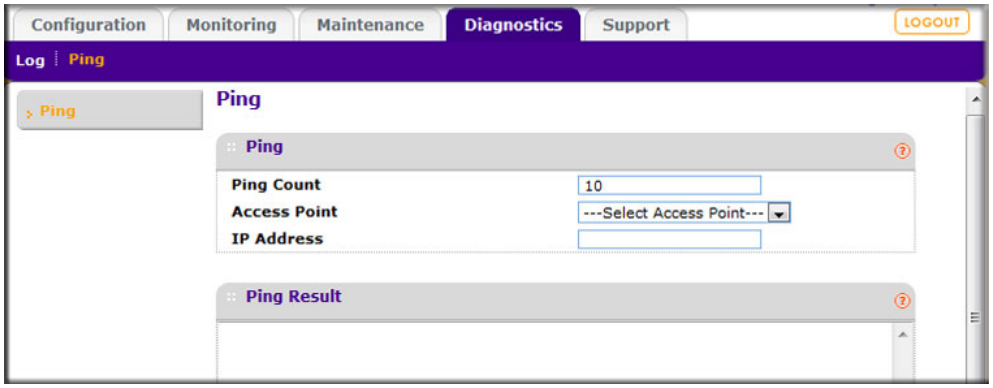
Select one of the managed access points to display the system log.

Note: Access point system logs are not supported for access point model WG602v4. If you try to display system logs for that model access point, the display screen is empty.

You can refresh the screen by using the **Refresh** button.

Diagnostic Ping Screen

This screen provides a way to verify ping connectivity from the wireless management system to a managed access point. Select a managed access point from the drop-down list. The IP address of the access point to be pinged is displayed in the read-only IP Address field.



1. Specify the number of pings to be tried in the **Ping Count** field.
2. Click **Start** to begin pinging the selected access point.
3. When you are finished, click **Cancel** to stop the pinging.

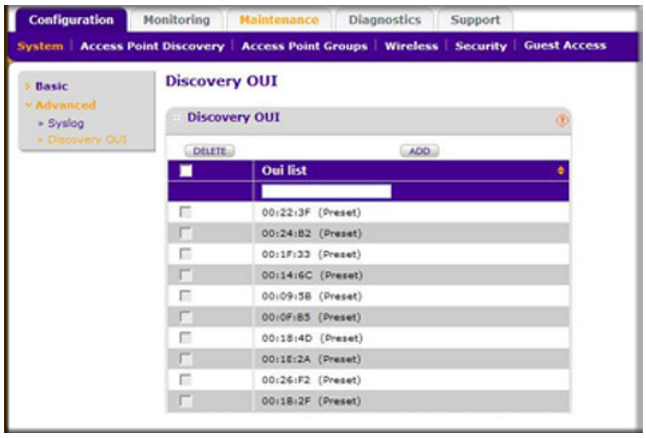
Using Discovery OUI

The wireless management system discovers NETGEAR access points on the LAN from the OUI (Organizationally Unique Identifier) of their unique MAC addresses. The first half of the MAC address is the OUI. Usually, the wireless management system identifies the OUI without incident during discovery. OUIs are allocated to businesses that produce products with MAC addresses.

Discovery OUI is not often needed, but is useful in the following circumstances:

- There is a new NETGEAR access point that has a new OUI.
- The WMS5316 controller is running older firmware that does not recognize the new OUI.
- You do not want to update the WMS5316 firmware.

You can use Discovery OUI to register and discover the access point. On the Configuiration taba, select System > Advanced > Discovery OUI:



To change the settings:

1. Click **Add** or **Delete** to add or delete a OUI into the list.

> **Note:** OUIs already allocated for NETGEAR devices are preconfigured and cannot be deleted.

2. Click the **Apply** button to save your changes.

Access Point Firmware Compatibility

A

Compatible Access Point Supported Firmware Versions

Access Point Model	Supported Firmware	Security Profiles per Radio	Max Station Load Balancing	Auto Channel
WNDAP330	WNDAP330_V3.0.4	8	Yes	Yes
WNDAP350	WNDAP350_V2.0	8	Yes	Yes
WNAP210	WNAP210_2.0.8	8	Yes	Yes
WG302v2	5.2.3	8	No	Yes
WG103	WG103_2.0	8	Yes	No
WN802Tv2	WN802Tv2_V3.1.2	1	No	Limited to channel distribution without neighbor map
WG602v4	V1.1.0	1	No	Limited to channel distribution without neighbor map

For the latest firmware images, visit the NETGEAR support website: *http://www.netgear.com*.

Controller Features and Access Point Compatibility

Access Point Model	Topology	VLAN Config	Rogue Access Points	Remote Access SSH Telnet	Guest Access	Client Separation	Syslog	NTP (Time Server)
WNDAP330	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
WNDAP350	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WNAP210	Yes	Yes	Yes	Yes	Yes	Yes	SNS	Yes
WG302v2	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
WG103	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WN802Tv2	No	No	No	No	No	Yes	Yes	Yes
WG602v4	No	No	No	No	No	No	No	No
WNDAP330	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

Factory Default Settings

B

You can use Reset option to restore the wireless management system to its factory default settings (see *Restoring Factory Default Settings* on page 47). The wireless management system will return to the factory configuration settings shown in the following table.

Table 4. Factory Default Settings

Feature		Default Behavior
Login	User login URL	http:192.168.0.250
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Local network (LAN)	LAN IP	192.168.0.250
	Subnet mask	255.255.255.0
	Time zone	PST for North America, GMT for other locations
	Time zone adjusted for daylight savings time	Enabled
	SNMP	Enabled

For technical specifications, see the NETGEAR website at *www.netgear.com*.

Notification of Compliance

NETGEAR Wired Products

C

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe™ 16 AP Wireless Management System WMS5316 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe™ 16 AP Wireless Management System WMS5316 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

CE

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

For complete DoC please visit the NETGEAR EU Declarations of Conformity website at:
http://kb.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.

EDOC in Languages of the European Community

Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, Santa Clara, CA 95134, declare under our sole responsibility that the ProSafe™ 16 AP Wireless Management System WMS5316 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful

interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

ProSafe™ 16 AP Wireless Management System

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE
PY306100037

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, (ProSafe™ 16 AP Wireless Management System WMS5316), does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-FVX538

Index

A

access point groups 44
  WLAN settings 18
access point system logs 56
access points
  adding 16
  discovery 13, 14
  discovery results 15
  passwords 16
  rogue 27, 35
  status 34, 36, 37
  supported firmware 58
  upgrading firmware 52
access, guest 32
adding access points 16
authentication, MAC 28
Auto Discovery 13

B

backing up 54

C

centralized RF management 17
clients, status 38
compliance 61
configuration settings 54

D

DHCP leases 40
DHCP server 11
diagnostics, ping 56
discovering access points 13
  Auto Discovery 13
  IP Discovery 14
  results 15
Discovery OUI 57
DNS server 9

F

firmware
  access point supported 58
  upgrading 51
  upgrading access point firmware 52

G

general settings 7
groups 44
  editing access point information 43
  IP settings 44
  MAC authentication 29
guest access 32
  show 33

I

IP address 9, 60
IP discovery 14
IP settings 9
  access point groups 44

L

leases, DHCP 40
load balancing 22, 23
logging in to the Wireless Management System 7
logs
  access point 56
  downloading 55
  system 55

M

MAC authentication 28, 29
Managed Access Point List 42
management VLANs 10
monitoring
  client status 38
  network usage 36, 39
monitoring summary 34, 42, 45

N

network topology 39
network usage 36, 39

network usage statistics 39

O

OUI Discovery 57

P

passwords 7
  changing 46
  for access points 16
ping 56

Q

QoS 21, 22

R

RADIUS server configuration 31, 32
rebooting 46, 48
remote console 50
remote console for access point groups 50
remote management 50
resetting 46
restoring
  configuration settings from a file 54
  factory default settings 47
RF management, centralized 17
rogue access points 27, 35

S

security profiles
  editing 25
  for access point groups 26
  list 24
session timeout 51
SNMP 48, 49
statistics, network usage 39
status
  access points 34, 36, 37
  client 38
  wireless stations 35
subnet mask 9, 60
Syslog 12
system logs 55
  access point 56

T

technical support 2
time, setting 8
timeout 51
trademarks 2

U

untagged VLANs 10
upgrading firmware 51

V

VLANS 10
VLANs 9, 10

W

wireless access point groups 18
wireless centralized RF management 17
wireless station status 35